明 細 書

素数算出装置及び方法並びに鍵発行システム

技術分野

[0001] 本発明は、素因数分解の困難さを安全性の根拠として情報のセキュリティを保持する技術に関する。

背景技術

[0002] 近年、コンピュータ技術及び通信技術に基づくデータ通信が広く普及してきており、このデータ通信においては、秘密通信方式やデジタル署名方式が用いられる。ここで、秘密通信方式とは、特定の通信相手以外に通信内容を漏らすことなく通信を行う方式である。またデジタル署名方式とは、通信相手に通信内容の正当性を示したり、発信者の身元を証明したりする通信方式である。

[0003] 1. 公開鍵暗号方式

これらの秘密通信方式又はデジタル署名方式においては、公開鍵暗号方式とよばれる暗号方式が用いられる。公開鍵暗号方式を用いる秘密通信では、暗号化鍵と復号化鍵とが異なり、復号化鍵は秘密にするが、暗号化鍵は公開する。秘密にする復号化鍵を秘密鍵と呼び、公開する暗号化鍵を公開鍵と呼ぶ。通信相手が多数のとき、共通鍵暗号では通信相手間で鍵をもつ必要があるが、公開鍵暗号では通信相手が一つの固有の鍵をもつだけで通信可能になるため、通信相手が増えても、共通鍵暗号より鍵の数が少なくてよい。このように、公開鍵暗号は多数の通信相手と通信を行うのに適しており、不可欠な基盤技術である。

[0004] 公開鍵暗号方式の1種であるRSA暗号方式では、整数の素因数分解問題を解くことが、計算量の上で困難であることを安全性の根拠としている。素因数分解問題とは、p, qを素数とし、整数n＝p×qとするとき、整数nに対して、素数p, qを求める問題である。ここで、×は通常の乗算である。一般にp, qが1024ビットの数のように大きい場合は、素因数分解問題が困難である。それにより、RSA暗号方式の公開鍵から秘密鍵を求めることや、秘密鍵を持たないユーザが暗号文から平文を求めることが、困難になる。なお、素因数分解問題については、非特許文献1の144ー151ページに

詳しく述べられている。

[0005] (素因数分解問題を応用するRSA暗号方式)

ここで、素因数分解問題を応用するRSA暗号方式について説明する。

(1)鍵の生成

次に示すようにして公開鍵及び秘密鍵を計算する。

・ランダムに大きい素数p, qを選択し、その積n＝p×qを計算する。

[0006] ・(p−1)及び(q−1)の最小公倍数L＝LCM(p−1, q−1)を計算する。

・Lと互いに素でLより小さい自然数eをランダムに選ぶ。

$$1 \leqq e \leqq L-1,\ GCD(e, L) = 1$$

ここで、GCD(e, L)は、eとLの最大公約数を示している。

・e×d＝1 mod Lを満たすdを計算する。GCD(e, L)＝1より、このようなdは必ず存在する。このようにして、得られた整数e及び整数nが、公開鍵である。また、整数dが、秘密鍵である。ここで、x mod yは、xをyで割った余りを示す。

[0007] (2)暗号文の生成

公開鍵である整数e及び整数nを用いて、平文mに暗号演算を施して暗号文cを計算する。

$$c = m^{\wedge} e \mod n$$

なお、この明細書において、演算子^は、べき乗を示す。例えば、A^xは、x＞0のときはAをx回乗じたものを示す。

[0008] (3)復号文の生成

秘密鍵である整数dを用いて、暗号文cに復号演算を施して復号文m'を計算する。

$$m' = c^{\wedge} d \mod n$$

なお、

$$\begin{aligned} m' &= c^{\wedge} d \mod n \\ &= (m^{\wedge} e)^{\wedge} d \mod n \\ &= m^{\wedge}(e \times d \mod L) \mod n \\ &= m^{\wedge} 1 \mod n \\ &= m \mod n \end{aligned}$$

であるので、復号文m'は、平文mと一致する。

[0009] また、RSA暗号については、非特許文献2の110ー113ページに詳しく説明されている。

上記に示した素因数分解を応用したRSA暗号における公開鍵の生成のステップにおいて、素数生成が行われる。素数生成については、非特許文献3の145ー154ページに詳しく説明されている。素数生成方法には、確率的素数生成法と確定的素数生成方法がある。確率的素数生成法により生成される素数は、「素数である確率が高い」数であり、100%素数であるとは限らない。一方、確定的素数生成方法は、確実に素数である数を生成する。確率的素数生成方法及び確定的素数生成方法については、非特許文献2に詳しく説明されている。以下では、確定的素数生成方法について説明する。

[0010] 2. 従来例1ー確定的素数生成方法

確定的に素数を生成することができるMaurer法による確定的素数生成方法について説明する。ここで、Maurer法については、非特許文献3の152ー153ページに詳しく説明されている。

前記確定的素数生成方法では、次に示すステップを繰り返すことにより、素数を生成する。あらかじめビットサイズlenqの素数qが与えられている。

[0011] (ステップ1)(lenq−1)ビットの乱数Rを選択する。なお、乱数Rの先頭ビットは、必ず1となるようにする。

(ステップ2)数Nを以下の式により計算する。

$$N=2\times q\times R+1$$

(ステップ3)数Nが素数であるか否かを、次に示す第1判定及び第2判定がともに、成立する場合に、素数と判定する。他の場合に、素数でないと判定する。

[0012] (第1判定) $2^{(N-1)} = 1 \mod N$

(第2判定) $GCD(2^{(2R)}-1, N)=1$

素数であると判定される場合には、数Nを素数として出力する。素数でないと判定される場合には、ステップ1へ戻って、素数が出力されるまで、処理を繰り返す。

ステップ3で述べられている判定方法は、Pocklingtonの素数判定法とよばれ、非

特許文献3の144ページに詳しく述べられている。Pocklingtonの素数判定法では、N＝2×q×R＋1のqが素数であり、第1判定及び第2判定の結果が真であれば、必ず、Nが素数になる。そのため、確定的に素数であることを判定でき、確定的な素数生成が可能になる。

[0013] このようにして、Maurer法による確定的素数生成方法では、サイズlenqの素数qを基にして、サイズ2×lenqの素数Nを生成する。従って、Maurer法による確定的素数生成方法を用いて所定長の素数を生成する場合には、前記所定長以下の素数の生成を繰り返し行う。例えば、512ビット長の素数を生成する場合には、あらかじめ与えられた8ビットの素数を基にして16ビットの素数を生成する。次に、生成した16ビットの素数を基にして32ビットの素数を生成する。次に、生成した32ビットの素数を基にして64ビットの素数を生成する。以下同様の素数生成を繰り返して、512ビットの素数を生成する。

[0014] なお、前記第2判定を次の判定に代えてもよい。

（第3判定） $2^{(2R)} \neq 1 \mod N$

上記第3判定方法は、非特許文献4に詳しく述べられている。以降、こちらの判定方法を使用していく。

3. 複数の鍵発行サーバをもつ鍵発行システム

公開鍵暗号の鍵発行システムでは、ユーザが鍵を生成する場合や、鍵発行サーバによりユーザに鍵を発行する場合がある。鍵発行サーバにより鍵を発行する場合、ユーザに鍵を発行するサーバは一台であることが多い。しかし、処理の負荷を軽減するために、鍵発行システムは、複数台の鍵管理サーバを備え、複数台の鍵管理サーバのそれぞれにおいて、鍵を発行することもある。

特許文献1:特開2003−5644号公報

非特許文献1:岡本龍明、太田和夫共編、「暗号・ゼロ知識問題・数論」、共立出版、1990

非特許文献2:岡本龍明、山本博資、"現代暗号"、産業図書(1997年)

非特許文献3:A. J. Menezes, P. C. van Oorschot, S. A. Vanstone, "Handbook of applied cryptography", CRC Pres s, 1997

非特許文献4:岡本 栄司、「暗号理論入門」、共立出版、1993、21ページ

非特許文献5:Henri Cohen, "A Course in Computational Algebraic Number Theory", GTM 138, Springer—Verlag, 1993

発明の開示

発明が解決しようとする課題

[0015] 複数台の鍵発行サーバを用いた鍵発行システムでは、第1の鍵発行サーバと、第2の鍵発行サーバにおいて、それぞれ発行したRSA鍵を互いにチェックすることはない。なぜなら、発行したRSA鍵を、他の鍵発行サーバへ公開すると、セキュリティ上問題があるからである。このため、偶然、第1及び第2の鍵発行サーバが、第1のユーザ及び第2のユーザのために、同じ公開鍵と同じ秘密鍵を生成することが起こりうる。

[0016] このため、暗号方式を利用する際に、セキュリティが確保できないという問題がある。

例えば、第3のユーザが、第1のユーザのための前記公開鍵を用いて、第1のユーザに対して、暗号文を生成して送付すると、第1のユーザは、当然、自身の秘密鍵を用いて、暗号文を復号できるが、第2のユーザも自身の秘密鍵を用いて、前記暗号文を復号できてしまう。

課題を解決するための手段

[0017] このような問題を解決するためには、RSAの公開鍵は、2つの異なる素数の積により演算されるので、公開鍵の生成において用いられる各素数が、第1の鍵発行サーバと、第2の鍵発行サーバにおいて、異なるようにしておけばよい。

そこで、本発明は、素数の算出を行う際に、簡単な管理により重複を避けながら素数を算出する素数算出装置、鍵発行システム、素数算出方法及び素数算出プログラムを提供することを目的とする。

[0018] 上記目的を達成するために、本発明は、既知の素数qより大きい素数候補Nを算出して素数判定する素数算出装置であって、既知の素数qを記憶している素数記憶手段と、素数の利用範囲における一意の管理情報を記憶している管理情報記憶手段と、前記管理情報記憶手段から前記管理情報を読み出し、読み出した前記管理情報に依存する攪乱情報Rを生成する攪乱情報生成手段と、前記素数記憶手段から前

記素数qを読み出し、読み出した前記素数q及び生成された前記攪乱情報Rを用いて、N＝2×攪乱情報R×素数q＋1により、素数候補Nを算出する候補算出手段と、算出された素数候補Nが素数であるか否かを判定する素数判定手段と、素数であると判定される場合に、算出された素数候補Nを素数として出力する出力手段とを備えることを特徴とする。

発明の効果

[0019] 上記に示した構成によると、素数算出装置は、一意の管理情報に依存して生成された攪乱情報Rを用いて、素数候補Nを算出するので、重複を避けながら素数候補を算出することができる。素数の利用範囲とは、素因数分解の困難性を安全性の根拠として素数を利用する範囲である。

ここで、前記攪乱情報生成手段は、前記管理情報記憶手段から前記管理情報を読み出す読出部と、乱数rを算出する乱数算出部と、読み出した前記管理情報と生成した乱数rとを結合する結合部と、前記管理情報と乱数rとの結合体に基づいて、攪乱情報Rを算出する演算部とを含むとしてもよい。

[0020] この構成によると、素数算出装置は、管理情報と乱数rとの結合体に基づいて、攪乱情報Rを生成するので、管理情報による一意性と、乱数rによるランダム性とを兼ね備えた攪乱情報を生成することができる。

ここで、前記演算部は、前記結合体に、単射の関数を施して攪乱情報Rを生成するとしてもよい。

[0021] この構成によると、素数算出装置は、結合体に、単射の関数を施して、攪乱情報Rを生成するので、単射の関数の性質により、結合体が有する一意性を保ち、且つ結合体から変換されることによるランダム性を備える攪乱情報を生成することができる。

ここで、前記単射の関数は、排他的論理和であり、前記演算部は、所定の鍵情報を予め記憶しており、前記鍵情報と前記結合体とに排他的論理和を施して攪乱情報Rを生成するとしてもよい。

[0022] この構成によると、素数算出装置は、結合体と所定の鍵情報とから、排他的論理和を施して、攪乱情報Rを生成することができる。

ここで、前記素数算出装置は、素数qの2倍のビット長を有する素数候補Nを算出し

、前記乱数算出部は、素数qのビット長から前記管理情報のビット長及び1を差し引いて得られるビット長の前記乱数rを算出するとしてもよい。

[0023] この構成によると、素数算出装置は、素数qのビット長から管理情報のビット長を及び1を差し引いて得られるビット長の乱数rを算出し、素数qの2倍のビット長を有する素数候補Nを算出することができる。

ここで、前記素数判定手段は、前記素数候補Nに対して、$2^{N-1}=1 \mod N$を満たすか否かを判定する第1判定部と、前記第1判定部により満たすと判定される場合に、さらに、素数候補N及び攪乱情報Rに対して、$2^{2R} \neq 1 \mod N$を満たすか否かを判定し、満たすと判定する場合に、素数候補Nが素数であると決定する第2判定部とを含むとしてもよい。

[0024] この構成によると、素数算出装置は、第1及び第2判定部を用いて、素数候補Nが素数であるか否かを判断するので、第1及び第2判定部の双方にて、判定結果が肯定的な場合に、素数候補Nを素数と判断することができる。

ここで、前記素数判定手段は、前記素数候補Nに対して、$2^{N-1}=1 \mod N$を満たすか否かを判定する第1判定部と、前記第1判定部により満たすと判定される場合に、さらに、素数候補N及び攪乱情報Rに対して、$GCD(2^{2R}-1, N)=1$を満たすか否かを判定し、満たすと判定する場合に、素数候補Nが素数であると決定する第2判定部とを含むとしてもよい。

[0025] この構成によると、素数算出装置は、第1及び第2判定部を用いて、素数候補Nが素数であるか否かを判断するので、第1及び第2判定部の双方にて、判定結果が肯定的な場合に、素数候補Nを素数と判断することができる。

ここで、前記素数算出装置は、さらに、前記素数判定手段により素数であると判定されるまで、前記攪乱情報生成手段、前記候補算出手段及び前記素数判定手段に対して、攪乱情報Rの生成と、素数候補Nの算出と、前記判定とを繰り返すように制御する繰返制御手段を含むとしてもよい。

[0026] この構成によると、素数算出装置は、繰返制御手段により、生成された素数候補が素数であると判定されるまで、攪乱情報Rの生成、素数候補Nの算出、素数の判定とを繰り返すので、常に、素数を出力することができる。

ここで、前記素数算出装置は、さらに、乱数R'を算出する次段乱数算出手段と、出力された前記素数N及び生成された前記乱数R'を用いて、N'＝2×乱数R'×素数N＋1により、素数候補N'を算出する次段候補算出手段と、算出された素数候補N'が素数であるか否かを判定する次段素数判定手段と、素数であると判定される場合に、算出された素数候補N'を素数として出力する次段出力手段と、前記次段素数判定手段により素数であると判定されるまで、前記次段乱数算出手段、前記次段候補算出手段及び前記次段素数判定手段に対して、乱数R'の生成と、素数候補N'の算出と、前記判定とを繰り返すように制御する次段繰返制御手段とを含むとしてもよい。

[0027] この構成によると、素数算出装置は、素数Nと、生成された乱数R'とを用いて、素数候補N'を算出し、算出された素数候補N'が素数であるか否かを判断し、素数である場合には、算出された素数候補N'を素数として出力することができる。

ここで、記素数算出装置は、さらに、所定の検証値を記憶している次段情報記憶手段と、乱数r'を生成する次段乱数生成手段と、前記管理情報に生成した前記乱数r'を乗じて攪乱情報R'を算出し、N'＝2×攪乱情報R'×素数N＋検証値により、素数候補N'を算出する次段候補算出手段とを含み、前記素数判定手段は、さらに、算出された素数候補N'が素数であるか否かを判定し、前記出力手段は、さらに、素数候補N'が素数であると判定される場合に、算出された素数候補N'を素数として出力するとしてもよい。

[0028] この構成によると、素数算出装置は、検証値と、素数Nと、管理情報に乱数r'を乗じた攪乱情報R'とを用いて、素数候補N'を算出し、算出された素数候補N'が素数であるか否かを判断し、素数である場合には、素数候補N'を素数として出力することができる。これにより、素数N'から検証値を減じた結果が、管理情報にて割り切れる素数N'を生成することができる。

[0029] ここで、前記素数算出装置は、RSA暗号の公開鍵及び秘密鍵を生成する鍵生成装置であり、前記素数算出装置は、さらに、算出された素数Nを用いて、RSA暗号の公開鍵を生成する公開鍵生成手段と、生成された公開鍵を用いて、RSA暗号の秘密鍵を生成する秘密鍵生成手段とを含むとしてもよい。

この構成によると、素数算出装置は、RSA暗号の公開鍵及び秘密鍵を生成する鍵

生成装置とすることができ、素数算出装置は、算出された素数Nを用いて、公開鍵を生成し、生成した公開鍵を用いて、秘密鍵を生成することができる。

[0030] ここで、前記公開鍵生成手段は、前記繰返制御手段に対して、新たに素数N'が得られるように指示し、前記素数N及び新たに得られた素数N'を用いて、n＝素数N×素数N'により、数nを算出し、乱数eを生成し、算出された数nと生成された乱数eとの組が前記公開鍵であり、前記秘密鍵生成手段は、e×d＝1 mod Lを満たすdを算出し、Lは、素数N−1と素数N'−1との最小公倍数であり、算出されたdが前記秘密鍵であるとしてもよい。

[0031] この構成によると、素数算出装置は、素数N及び素数N'を用いて、数nを算出し、乱数eを生成することにより、公開鍵を生成し、生成された乱数eと、素数N−1と素数N'−1との最小公倍数とから、秘密鍵を生成することができる。

ここで、前記素数算出装置は、端末装置に対して、RSAの秘密鍵及び公開鍵を生成し、発行する鍵発行サーバ装置であり、前記素数算出装置は、さらに、生成した前記秘密鍵を、端末装置に対して出力する鍵出力手段と、生成した前記公開鍵を、公開する公開手段とを含むとしてもよい。

[0032] この構成によると、素数算出装置は、生成した秘密鍵を端末装置に対して出力し、生成した公開鍵を公開することができる。

ここで、前記素数算出装置は、さらに、前記端末装置を一意に識別する端末装置識別子を取得する識別子取得手段と、取得した端末装置識別子を含む前記管理情報を生成する管理情報生成手段と、生成した前記管理情報を前記管理情報記憶手段に書き込む書込手段とを含むとしてもよい。

[0033] この構成によると、素数算出装置は、端末装置識別子を含む管理情報を生成し、生成した管理情報を管理情報記憶手段へ書き込むので、一意の管理情報を記憶することができる。

ここで、前記素数算出装置は、さらに、鍵発行サーバ装置としての当該素数算出装置を一意に識別するサーバ識別子を予め記憶しているサーバ識別子記憶手段を含み、前記管理情報生成手段は、さらに、前記サーバ識別子記憶手段から前記サーバ識別子を読み出し、読み出したサーバ識別子をさらに含む前記管理情報を生成

するとしてもよい。

[0034] この構成によると、素数算出装置は、さらに、サーバ識別子を含む管理情報を生成するので、管理情報の一意性を高めることができる。

また、本発明は、既知の素数より大きい素数を算出する素数算出装置であって、既知の入力素数の2倍のビット長を有する出力素数を算出する素数算出手段と、既知の素数初期値を記憶している素数記憶手段と、前記素数算出手段に対して、算出を複数回繰り返すように制御する繰返制御手段とを備え、前記繰返制御手段は、前記繰返しにおける初回の算出において、前記素数記憶手段に記憶されている素数初期値を、前記入力素数として、前記素数算出手段に与え、前記繰返しの初回の算出以外の他の算出において、1つ前の回の算出においてされた出力素数を、当該他の算出における前記入力素数として、前記素数算出手段に与え、前記複数回の算出のいずれか1の算出において、前記素数算出手段は、素数の利用範囲における一意の管理情報を記憶している管理情報記憶部と、前記管理情報記憶部から前記管理情報を読み出し、読み出した前記管理情報に依存する攪乱情報Rを生成する攪乱情報生成部と、前記入力素数qを受け取り、受け取った前記入力素数q及び生成された前記攪乱情報Rを用いて、N＝2×攪乱情報R×素数q＋1により、素数候補Nを算出する候補算出部と、算出された素数候補Nが素数であるか否かを判定する素数判定部と、素数であると判定される場合に、算出された素数候補Nを出力素数として出力する出力部と、前記素数判定部により素数であると判定されるまで、前記攪乱情報生成部、前記候補算出部及び前記素数判定部に対して、攪乱情報Rの生成と、素数候補Nの算出と、前記判定とを繰り返すように制御する繰返制御部とを含むことを特徴とする。

[0035] この構成によると、素数算出装置の素数出力手段は、複数回の出力素数の算出の何れかの1の算出において、一意の管理情報に依存して生成された攪乱情報Rを用いて、素数候補Nを算出するので、重複を避けながら素数候補を算出することができる。

ここで、前記複数回の算出のうち、最終回の算出において、前記素数算出手段は、所定の検証値を記憶している情報記憶部と、乱数r'を生成する乱数生成部と、前記

管理情報に生成した前記乱数r'を乗じて攪乱情報R'を算出し、N'＝2×攪乱情報R'×1つ前の回において算出された出力素数＋検証値により、素数候補N'を算出する候補算出部と、算出された素数候補N'が素数であるか否かを判定する素数判定部と、素数候補N'が素数であると判定される場合に、算出された素数候補N'を素数として出力する出力部と、前記素数判定部により素数であると判定されるまで、前記乱数生成部、前記候補算出部及び前記素数判定部に対して、乱数r'の生成と、素数候補N'の算出と、前記判定とを繰り返すように制御する繰返制御部とを含むとしてもよい。

[0036] この構成によると、素数算出装置は、検証値と、1つ前の回において算出された出力素数と、管理情報に乱数r'を乗じた攪乱情報R'とを用いて、素数候補N'を算出し、算出された素数候補N'が素数であるか否かを判断し、素数である場合には、素数候補N'を素数として出力することができる。これにより、素数N'から検証値を減じた結果が、管理情報にて割り切れる素数N'を生成することができる。

[0037] また、本発明は、端末装置に対してRSAの秘密鍵及び公開鍵を生成して発行する鍵発行サーバ装置と、前記端末装置とから構成される鍵発行システムであって、鍵発行サーバ装置は、既知の素数qより大きい素数Nを算出する素数算出手段と、算出された素数Nを用いて、RSA暗号の公開鍵を生成する公開鍵生成手段と、生成された公開鍵を用いて、RSA暗号の秘密鍵を生成する秘密鍵生成手段と、生成された前記秘密鍵を、端末装置に対して出力する鍵出力手段と、生成された前記公開鍵を公開する公開手段とを備え、前記素数算出手段は、既知の素数qを記憶している素数記憶部と、一意の管理情報を記憶している管理情報記憶部と、前記管理情報記憶部から前記管理情報を読み出し、読み出した前記管理情報に依存する攪乱情報Rを生成する攪乱情報生成部と、前記素数記憶部から前記素数qを読み出し、読み出した前記素数q及び生成された前記攪乱情報Rを用いて、N＝2×攪乱情報R×素数q＋1により、素数候補Nを算出する候補算出部と、算出された素数候補Nが素数であるか否かを判定する素数判定部と、素数であると判定される場合に、算出された素数候補Nを素数として出力する出力部と、前記素数判定部により素数であると判定されるまで、前記攪乱情報生成部、前記候補算出部及び前記素数判定部に対

して、攪乱情報Rの生成と、素数候補Nの算出と、前記判定とを繰り返すように制御する繰返制御部とを含み、前記端末装置は、前記秘密鍵を受け取る受信手段と、受信した秘密鍵を記憶する鍵記憶手段とを備えることを特徴とする。

[0038] この構成によると、鍵発行システムの鍵発行サーバ装置は、一意の管理情報に依存して生成された攪乱情報Rを用いて、素数候補Nを算出するので、重複を避けながら素数候補を算出することができる。端末装置は、秘密鍵を、鍵発行サーバ装置から受信し、記憶するので、重複を避けながら生成された素数Nにより生成された、つまり重複を避けながら生成された秘密鍵を記憶することができる。

[0039] ここで、前記鍵発行システムは、さらに、証明書発行サーバ装置を含み、前記鍵出力手段は、前記公開鍵を前記証明書発行サーバ装置へ出力し、前記証明書発行サーバ装置は、当該証明書発行サーバ装置の秘密鍵を記憶している記憶手段と、前記公開鍵を取得する取得手段と、前記証明書発行サーバ装置の秘密鍵を用いて、前記公開鍵を含む公開鍵情報に、デジタル署名を施して、署名データを生成し、少なくとも前記公開鍵及び生成した前記署名データを含む公開鍵証明書を生成する証明書生成手段と、生成した公開鍵証明書を鍵発行サーバ装置へ出力する出力手段とを備えるとしてもよい。

[0040] この構成によると、鍵発行システムは、証明書発行サーバ装置を用いて、鍵発行サーバ装置にて発行された公開鍵に対する公開鍵証明書を発行することができる。

図面の簡単な説明

[0041] [図1]鍵発行システム1の全体の概要を示す図である。

[図2]鍵発行サーバ100の構成を示すブロック図である。

[図3]素数生成部116の構成を示すブロック図である。

[図4]制御情報テーブルT100のデータ構造の一例を示す図である。

[図5]素数情報生成部133の構成を示すブロック図である。

[図6]証明書発行サーバ200の構成を示すブロック図である。

[図7]検証値テーブルT200のデータ構造の一例を示す図である。

[図8]端末装置300の構成を示すブロック図である。

[図9]鍵発行システム1の動作概要を示す流れ図である。

[図10]鍵発行システム1における鍵依頼処理の動作を示す流れ図である。

[図11]鍵発行システム1における鍵発行処理の動作を示す流れ図である。図12へ続く。

[図12]鍵発行システム1における鍵発行処理の動作を示す流れ図である。図11から続き、図13へ続く。

[図13]鍵発行システム1における鍵発行処理の動作を示す流れ図である。図12から続き、図14へ続く。

[図14]鍵発行システム1における鍵発行処理の動作を示す流れ図である。図13から続く。

[図15]素数生成処理の動作を示す流れ図である。

[図16]素数候補生成処理の動作を示す流れ図である。図17へ続く。

[図17]素数候補生成処理の動作を示す流れ図である。図16から続く。

[図18]鍵発行システム1における証明書発行処理の動作を示す流れ図である。

[図19]素数情報生成部133Aの構成を示すブロック図である。

[図20]検証値テーブルT250のデータ構造の一例を示す図である。

[図21]素数情報生成部133Bの構成を示すブロック図である。

[図22]素数生成部116Cの構成を示すブロック図である。

[図23]制御情報テーブルT150のデータ構造の一例を示す図である。

[図24]素数情報生成部133Cの構成を示すブロック図である。

[図25]素数候補生成処理の動作を示す流れ図である。

[図26]鍵発行システム2の全体の概要を示す図である。

[図27]鍵発行サーバ1100の構成を示すブロック図である。

[図28]発行済鍵情報テーブルT1100のデータ構造の一例を示す図である。

[図29]鍵発行監査サーバ1200の構成を示すブロック図である。

[図30]検証値テーブルT1200のデータ構造の一例を示す図である。

[図31]鍵発行時における鍵発行システム2の動作概要を示す流れ図である。

[図32]鍵監査時における鍵発行システム2の動作概要を示す流れ図である。

[図33]鍵発行システム2における証明書発行処理の動作を示す流れ図である。

[図34]鍵発行システム2における鍵情報取得処理の動作を示す流れ図である。

[図35]鍵発行システム2における監査処理の動作を示す流れ図である。

[図36]確認処理の動作を示す流れ図である。

[図37]8ビットの素数から512ビットの素数を生成するの動作を示す図である。

[図38]素数生成装置2100の構成を示すブロック図である。

[図39]素数生成処理の動作を示す流れ図である。

[図40]素数候補生成処理の動作を示す流れ図である。

[図41]素数生成装置2200の構成を示すブロック図である。

[図42]素数生成装置2300の構成を示すブロック図である。

[図43]素数生成装置2400の構成を示すブロック図である。

[図44]素数生成装置2500の構成を示すブロック図である。

[図45]発行識別子情報「IDI」のビット列に、乱数「R1」を構成する各ビットを埋め込んだ結果「IDI_R1」の一例を示す図である。

[図46]検証処理の動作を示す流れ図である。

符号の説明

[0042] 1 鍵発行システム

100、101、102 鍵発行サーバ

110 識別子格納部

111 秘密鍵格納部

112 公開鍵格納部

113 証明書格納部

114 制御部

115 識別子生成部

116 素数生成部

117 鍵判定部

118 鍵生成部

119 情報取得部

120 受信部

121 送信部

130 サーバ識別子記憶領域

131 端末情報記憶領域

132 繰返制御部

133 素数情報生成部

135 繰返カウンタ

136 出力カウンタ

140 情報制御部

141 乱数生成部

142 素数候補生成部

143 第1素数判定部

144 第2素数判定部

200 証明書発行サーバ

210 秘密鍵格納部

211 発行公開鍵格納部

212 発行識別子情報格納部

213 公開鍵証明書格納部

214 発行公開鍵確認部

215 公開鍵証明書生成部

216 証明書取得部

217 受信部

218 送信部

220 サーバ情報記憶領域

221 確認情報記憶領域

300、301、302、303、304、305、306 端末装置

310 秘密鍵格納部

311 公開鍵証明書格納部

312 制御部

313 受付部

314 無線部

315 ベースバンド信号処理部

316 スピーカー

317 マイク

318 表示部

319 アンテナ

320 端末識別子記憶領域

400 端末装置

2 鍵発行システム

1100、1101、1102 鍵発行サーバ

1110 識別子格納部

1111 秘密鍵格納部

1112 公開鍵格納部

1113 証明書格納部

1114 制御部

1115 識別子生成部

1116 素数生成部

1117 鍵判定部

1118 鍵生成部

1119 情報取得部

1120 受信部

1121 送信部

1122 証明書生成部

1123 証明書用秘密鍵格納部

1124 発行済鍵情報格納部

1130 サーバ識別子記憶領域

1131 端末情報記憶領域

1200 鍵発行監査サーバ

1210 確認情報格納部

1211 発行済鍵情報格納部

1212 制御部

1213 発行公開鍵確認部

1214 受付部

1215 監査結果出力部

1216 受信部

1217 送信部

1220 サーバ情報記憶領域

1250 モニタ

1300、1301、1302、1303、1304、1305、1306 端末装置

1400 端末装置

2100 素数生成装置

2101 受付部

2102 受付情報記憶部

2103 素数シード生成部

2104 乱数生成部

2105 素数候補生成部

2106 素数判定部

2107 素数判定部

2200 素数生成装置

2201 受付部

2202 受付情報記憶部

2203 乱数生成部

2204 素数候補生成部

2205 素数判定部

2206 素数判定部

2300 素数生成装置

2301 受付部

2302 受付情報記憶部

2303 識別子素数生成部

2304 乱数生成部

2305 素数候補生成部

2306 素数判定部

2307 素数判定部

2400 素数生成装置

2401 受付部

2402 受付情報記憶部

2403 乱数生成部

2404 素数候補生成部

2405 素数判定部

2406 素数判定部

2500 素数生成装置

2501 受付部

2502 受付情報記憶部

2503 乱数生成部

2504 素数候補生成部

2505 素数判定部

2506 素数判定部

発明を実施するための最良の形態

[0043] 1. 第1の実施の形態

本発明に係る第1の実施の形態としての鍵発行システム1について、説明する。

1. 1 鍵発行システム1の概要

鍵発行システム1は、図1に示すように、鍵発行サーバ100、101、102と、証明書

発行サーバ200と、端末装置300、301、・・・、302、303、・・・、304、305、・・・、306とから構成されている。端末装置の台数は、例えば1000台である。

[0044] 鍵発行サーバ100、101及び102は、それぞれ異なる会社にて管理されている。端末装置300、301、・・・、302は、鍵発行サーバ100に対して、鍵の発行要求し、端末装置303、・・・、304は、鍵発行サーバ101に対して、鍵の発行要求し、端末装置305、・・・、306は、鍵発行サーバ102に対して、鍵の発行要求をする。なお、端末装置300、301、・・・、302は、鍵発行サーバ100との間には、安全な通信経路が確立されているものとする。また、端末装置303、・・・、304と、鍵発行サーバ101との間、及び端末装置305、・・・、306と、鍵発行サーバ102との間においても、同様に、安全な通信経路が確立されているものとする。

[0045] また、鍵発行サーバ100、101、102と、証明書発行サーバ200との間においても、同様に、安全な通信経路が確立されているものとする。

なお、以下においては、鍵発行サーバ100、証明書発行サーバ200、及び端末装置300を用いて、鍵発行システム1の概要を説明する。

鍵発行サーバ100は、端末装置300より鍵の発行要求を受け取ると、RSA暗号における秘密鍵及び公開鍵を生成し、証明書発行サーバ200に対して、生成した公開鍵に対する公開鍵証明書の発行要求をする。なお、ここで、生成する各鍵の鍵長は、1024ビットとする。

[0046] 証明書発行サーバ200は、鍵発行サーバ100より証明書の発行要求を受け取ると、公開鍵証明書を発行して、発行した公開鍵証明書を鍵発行サーバ100へ送信する。

鍵発行サーバ100は、証明書発行サーバ200より公開鍵証明書を受け取ると、受け取った公開鍵証明書と、生成した秘密鍵とを、端末装置300へ送信する。

端末装置300は、公開鍵証明書と、秘密鍵とを、鍵発行サーバ100より受け取ると、受け取った公開鍵証明書と、秘密鍵とを記憶する。

[0047] 以降、例えば、端末装置400のユーザは、先ず、鍵発行サーバ100より、端末装置300の公開鍵証明書を入手、又は端末装置300より公開鍵証明書を入手し、証明書発行サーバ200が有する公開鍵を用いて、公開鍵証明書の正当性を確認し、正当

な公開鍵証明書であると判断する場合に、入手した公開鍵証明書を、端末装置400にて記憶する。端末装置400は、記憶している公開鍵証明書に含まれる公開鍵を用いて、端末装置300へ送信する電子メールを暗号化して、暗号化された電子メールを端末装置300へ送信する。

[0048] 端末装置300は、端末装置400より暗号化された電子メールを受信すると、記憶している秘密鍵を用いて、暗号化された電子メールを復号して、復号された電子メールを表示する。

これにより、端末装置300と端末装置400との間では、安全にデータのやりとりができるようになる。

[0049] なお、端末装置301、・・・、302は、端末装置300と同様であるため、説明は省略する。また、鍵発行サーバ101、及び102は、鍵発行サーバ100と同様であるため、説明は省略する。

以降の説明において、各端末装置の代表として端末装置300を、各鍵発行サーバの代表として鍵発行サーバ100を用いる。

[0050] 1．2 鍵発行サーバ100の構成

鍵発行サーバ100は、図2にて示すように、識別子格納部110、秘密鍵格納部111、公開鍵格納部112、証明書格納部113、制御部114、識別子生成部115、素数生成部116、鍵判定部117、鍵生成部118、情報取得部119、受信部120及び送信部121から構成されている。

[0051] 鍵発行サーバ100は、具体的には、マイクロプロセッサ、ROM、RAM、ハードディスクユニット、ディスプレイユニット、キーボード、マウスなどから構成されるコンピュータシステムである。前記RAM又は前記ハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することにより、鍵発行サーバ100は、その機能を達成する。

[0052] なお、鍵発行サーバ101、及び102は、鍵発行サーバ100と同様の構成であるため、説明は省略する。

(1)識別子格納部110

識別子格納部110は、ビットサイズが126ビット以下である発行識別子情報を記憶

するための領域を有している。発行識別子情報のビットサイズは、例えば、64ビットである。

[0053] (2)秘密鍵格納部111

秘密鍵格納部111は、秘密鍵生成の際に用いられる2つの素数を記憶するための素数格納領域と、鍵生成部118にて生成された秘密鍵を記憶するための秘密鍵格納領域とを有している。

(3)公開鍵格納部112

公開鍵格納部112は、鍵生成部118にて生成された公開鍵を記憶するための領域を有している。

[0054] (4)証明書格納部113

証明書格納部113は、証明書発行サーバにて発行された公開鍵証明書を記憶する領域を有している。

(5)制御部114

制御部114は、図2に示すように、サーバ識別子記憶領域130と、端末情報記憶領域131とを有している。

[0055] サーバ識別子記憶領域130は、当該サーバを識別するサーバ識別子を予め記憶している。例えば、鍵発行サーバ100は、SIDAを、鍵発行サーバ101は、SIDBを、鍵発行サーバ102は、SIDCを記憶している。なお、以降では、鍵発行サーバ100のサーバサーバ識別子を「SID」として説明する。ここでは、サーバ識別子のビットサイズを31ビットとする。

[0056] 端末情報記憶領域131は、鍵発行の要求のあった端末装置を識別する端末識別子を記憶する領域を有している。ここで、端末識別子は、例えば、端末装置のシリアル番号である。ここでは、シリアル番号のビットサイズを32ビットする。

制御部114は、端末装置300から受信部120を介して、鍵の発行要求を示す鍵発行依頼情報と、端末装置300の端末識別子「TID」とを受け取ると、受け取った端末識別子「TID」を端末情報記憶領域131へ書き込む。制御部114は、発行識別子情報の生成命令と、受け取った端末識別子「TID」とを識別子生成部115へ出力する。

[0057] 制御部114は、証明書発行サーバ200から受信部120を介して、公開鍵証明書「

Cert」を受け取ると、受け取った公開鍵証明書「Cert」を証明書格納部113へ書き込む。制御部114は、秘密鍵及び公開鍵証明書を、鍵の発行要求のあった端末装置300へ配布の処理を開始する配布開始命令を情報取得部119へ出力する。

(6)識別子生成部115

識別子生成部115は、制御部114から発行識別子情報の生成命令と、端末識別子「TID」とを受け取ると、サーバ識別子記憶領域にて記憶されているサーバ識別子「SID」を取得する。

[0058] 識別子生成部115は、取得したサーバ識別子「SID」と、受け取った端末識別子「TID」と数「1」とから、発行識別子情報「IDI＝SID｜｜TID｜｜1」を生成する。ここで、記号「｜｜」はビットまたはバイト連結である。発行識別子情報「IDI」の最下位ビットを「1」とすることにより、発行識別子情報「IDI」は、常に奇数となり、そのビットサイズは、64ビットとなる。

[0059] 識別子生成部115は、生成した発行識別子情報「IDI」を識別子格納部110へ書き込み、素数生成部116へ、素数の生成開始命令を出力する。

(7)素数生成部116

素数生成部116は、図3に示すように、繰返制御部132及び素数情報生成部133とを有している。

[0060] 素数生成部116は、8ビットの素数から512ビットの素数を生成し、生成した512ビットの素数を鍵判定部117へ出力する。

＜繰返制御部132＞

繰返制御部132は、8ビットからなる素数とその素数のビットサイズ(つまり「8」)とを予め記憶している初期値記憶領域と、素数情報生成部133から受け取った素数を一時的に記憶する一時記憶領域とを有している。

[0061] 繰返制御部132は、図3に示すように、素数情報生成部133の動作の繰返回数をカウントする繰返カウンタ135と、鍵判定部117へ出力した素数の個数、つまり生成した512ビットの素数の出力回数をカウントする出力カウンタ136とを有している。なお、繰返カウンタ135及び出力カウンタ136の初期値は、それぞれ「1」である。

繰返制御部132は、図4に示す制御情報テーブルT100を有している。制御情報

テーブルT100は、回数と制御情報とからなる組を1以上格納している。回数は、繰返カウンタ135の値に対応する。制御情報は、素数情報生成部133にて生成する素数の生成方法の種別を示す。

[0062] 繰返制御部132は、識別子生成部115から素数の生成開始命令を受け取ると、素数情報生成部133が素数を生成するよう制御する。素数情報生成部133から素数を受け取ると、繰返カウンタ135及び出力カウンタ136のそれぞれの値に基づいて、再度、素数情報生成部133へ素数生成の命令、及び受け取った素数を鍵判定部117へ出力の何れかを行う。

[0063] 以下に、その動作について説明する。

繰返制御部132は、識別子生成部115から素数の生成開始命令を受け取ると、繰返カウンタ135及び出力カウンタ136を、それぞれ「1」に設定する。

繰返制御部132は、素数情報生成部133から、素数を受け取ると、繰返カウンタ135の値に「1」を加算し、加算結果が、7であるか否かを判断する。

[0064] 加算結果が7であると判断する場合には、繰返制御部132は、出力カウンタ136の値が、1であるか否かを判断する。1であると判断する場合には、繰返制御部132は、受け取った素数を素数「p1」として、鍵判定部117へ出力し、出力カウンタ136の値に「1」を加算し、繰返カウンタ135の値に「1」を設定する。1でない、つまり2以上であると判断する場合には、繰返制御部132は、受け取った素数を素数「p2」として、素数「p2」と判定開始命令を鍵判定部117へ出力する。

[0065] 加算結果が7でないと判断する場合には、受け取った素数のビットサイズを算出し、繰返制御部132は、受け取った素数と、算出したビットサイズとを、一時記憶領域に一時的に記憶する。

繰返制御部132は、素数の生成開始命令を受け取り、繰返カウンタ135及び出力カウンタ136のそれぞれの値に「1」を加算した後、素数情報生成部133から受け取った素数とそのビットサイズとを一時的に記憶した後、及び出力カウンタ136に「1」を加算し、且つ繰返カウンタ135の値を「1」に設定した後の何れかの場合において、繰返制御部132は、以下の動作を行う。

[0066] 繰返制御部132は、繰返カウンタ135の値が、1であるか否かを判断する。1である

と判断する場合には、初期値記憶領域より8ビットの素数とそのビットサイズを読み出し、1でないと判断する場合には、一時記憶領域よりビットサイズ「8×(2^(n−1))」と、その素数とを読み出す。つまり、繰返制御部132は、繰返カウンタ135の値が、1でないと判断する場合には、一時記憶領域より、直前に一時的に記憶した素数とそのビットサイズとを読み出す。ここで、「n」は、繰返カウンタの値である。これにより、繰返制御部132は、一時記憶領域より、前回生成した素数及びそのビットサイズを読み出す。例えば、繰返カウンタ135に値が「2」である場合には、繰返制御部132は、「16」ビットからなる素数を読み出し、繰返カウンタ135に値が「3」である場合には、「31」ビットからなる素数を読み出す。つまり、繰返カウンタ135の値が「2」から「6」までの間、順に、「16」ビットからなる素数、「32」ビットからなる素数、「64」ビットからなる素数、「128」ビットからなる素数、及び「256」ビットからなる素数を読み出すことになる。

[0067] 繰返カウンタ135の値に対応する制御情報を制御情報テーブルT100より読み出し、読み出した制御情報が、「情報C」であるか否かを判断する。

「情報C」であると判断する場合には、繰返制御部132は、読み出した素数及びそのビットサイズと、制御情報とからなる第1情報を生成し、生成した第1情報を、素数情報生成部133へ出力する。

[0068] 「情報C」でないと判断する場合には、繰返制御部132は、識別子格納部110より発行識別情報「IDI」を取得し、取得した発行識別子情報「IDI」のビットサイズ「lenIDI」を算出し、読み出した素数及びそのビットサイズと、制御情報と、発行識別子情報「IDI」及びそのビットサイズ「lenIDI」とからなる第2情報を生成し、生成した第2情報を、素数情報生成部133へ出力する。

[0069] また、繰返制御部132は、鍵判定部117より素数を再度生成する旨の再生成命令を受け取ると、出力カウンタ136の値に「1」を加算し、且つ繰返カウンタ135の値を「1」に設定し、繰返カウンタ135の値が、1であるか否かの判断を行う動作以降を行う。

＜素数情報生成部133＞

素数情報生成部133は、図5に示すように、情報制御部140、乱数生成部141、素数候補生成部142、第1素数判定部143及び第2素数判定部144から構成されている。

[0070] 素数情報生成部133は、繰返制御部132から受け取った素数のビットサイズが2倍のビットサイズからなる素数を生成する。例えば、8ビットからなる素数を受け取った場合には、16ビットからなる素数を生成し、16ビットからなる素数を受け取った場合には、32ビットからなる素数を生成する。

なお、以下の説明において、繰返制御部132から受け取る素数を素数「q」、そのビットサイズを「lenq」として、各構成要素について説明する。

[0071] ＜情報制御部140＞

情報制御部140は、第1情報及び第2情報を記憶するための情報記憶領域を有している。

情報制御部140は、証明書発行サーバ200により割り当てられ、且つ制御情報「情報A」に基づいて素数を生成する際に用いる第1検証値「c11」及び第2検証値「c12」を予め記憶している検証値記憶領域を有している。

[0072] 情報制御部140は、繰返制御部132から、素数「q」と、素数のビットサイズ「lenq」と、制御情報とからなる第1情報を受け取ると、受け取った第1情報を情報記憶領域へ書き込む。つまり、素数「q」と、素数のビットサイズ「lenq」と、制御情報（この場合、「情報C」）とを書き込む。

情報制御部140は、繰返制御部132から、素数「q」と、素数のビットサイズ「lenq」と、制御情報と、発行識別子情報「IDI」と、そのビットサイズ「lenIDI」とからなる第2情報を受け取ると、受け取った第2情報を情報記憶領域へ書き込む。つまり、素数「q」と、素数のビットサイズ「lenq」と、制御情報、発行識別子情報「IDI」と、そのビットサイズ「lenIDI」とを書き込む。

[0073] 情報制御部140は、受け取った情報の書き込み後、乱数の生成の指示を示す第1生成指示を、乱数生成部141へ出力する。

情報制御部140は、第2素数判定部144より、素数を受け取ると、受け取った素数を繰返制御部132へ出力する。

情報制御部140は、素数候補生成部142から出力カウンタ136の値を読み出す旨の回数読出命令を受け取ると、繰返制御部132の出力カウンタ136の値を読み出す。情報制御部140は、読み出した値を、素数候補生成部142へ出力する。

[0074] ＜乱数生成部141＞

乱数生成部141は、乱数の生成の指示を示す第1生成指示を、情報制御部140から受け取ると、情報制御部140の情報記憶領域にて記憶されている制御情報を読み出す。乱数生成部141は、読み出した制御情報が「情報C」であるか否かを判断する。

「情報C」であると判断する場合には、乱数生成部141は、情報制御部140の情報記憶領域にて記憶されている「lenq」を読み出し、(lenq−1)ビットからなる乱数「R1」を生成し、生成した乱数「R1」と読み出した制御情報とを素数候補生成部142へ出力する。ここで、乱数「R1」の最上位ビットは1とする。乱数生成方法は、非特許文献2が詳しい。

[0075] 「情報C」でないと判断する場合には、乱数生成部141は、情報制御部140の情報記憶領域にて記憶されている「lenq」及び「lenIDI」を読み出し、(lenq−lenIDI−1)ビットからなる乱数「R1」を生成し、生成した乱数「R1」と読み出した制御情報とを素数候補生成部142へ出力する。ここで、乱数「R1」の最上位ビットは1とする。

[0076] また、乱数生成部141は、第1素数判定部143及び第2素数判定部144の何れかから、再度乱数を生成する旨の第2生成指示を受け付けると、制御情報を情報記憶領域より読み出し、上記の動作を行う。

＜素数候補生成部142＞

素数候補生成部142は、生成された情報を記憶する生成情報記憶領域と、単射である関数「f」を予め記憶している関数記憶領域とを有している。ここで、関数「f」は、例えば、f(X||Y)＝Enc(K、X||Y)である。Enc(K、X||Y)は鍵Xを用いたときの(X||Y)の共通鍵暗号による暗号文である。共通鍵暗号の暗号化関数は一般的に全単射である。また、記号「||」はビットまたはバイト連結である。暗号化関数「Enc(K、X||Y)」の一例は、「Enc(K、X||Y)＝K XOR X||Y」である。なお、共通暗号の一例は、DESであり、DESを用いる場合には、鍵長は128ビットとなる。このとき、素数候補生成部142は、所定の鍵「K」を記憶している。

[0077] 素数候補生成部142は、乱数生成部141より、乱数「R1」と制御情報とを受け取ると、受け取った制御情報が「情報C」であるか否かの判断をする。

「情報C」であると判断する場合には、素数候補生成部142は、情報制御部140の情報記憶領域より素数「q」を読み出す。素数候補生成部142は、読み出した素数「q」と乱数生成部141より受け取った乱数「R1」とを用いて、数「N＝2×R1×q＋1」を生成する。このとき生成した数「N」が素数候補となる。

[0078] 素数候補生成部142は、生成した数「N」のビットサイズ「lenN」が「lenq」と一致するか否かを判断し、一致すると判断する場合には、素数候補生成部142は、生成した数「N」を第1素数判定部143へ出力し、受け取った乱数「R1」を、「R」として生成情報記憶領域に記憶する。

一致しないと判断する場合には、素数候補生成部142は、乱数生成部141より受け取った乱数「R1」に2を掛けて、その結果を「R1」として、再度、上記の動作を行い、数「N＝2×R1×q＋1」を生成する。

[0079] 制御情報が「情報C」でないと判断する場合には、素数候補生成部142は、情報制御部140の情報記憶領域より素数「q」及び発行識別子情報「IDI」を読み出す。素数候補生成部142は、制御情報が「情報B」であるか否かを判断する。

「情報B」であると判断する場合には、素数候補生成部142は、受け取った乱数「R1」と読み出した発行識別子情報「IDI」とから、結合値「IDI｜｜R1」を生成し、生成した結合値「IDI｜｜R1」と関数記憶領域にて記憶している関数「f」とを用いて、数「R＝f(IDI｜｜R1)」を生成する。素数候補生成部142は、生成した数「R」と読み出した素数「q」とを用いて、数「N＝2×R×q＋1」を生成する。このとき生成した数「N」が素数候補となる。

[0080] 素数候補生成部142は、生成した数「N」のビットサイズ「lenN」が「2×lenq」であるか否かを判断する。

「2×lenq」であると判断する場合には、素数候補生成部142は、生成した数「N」を第1素数判定部143へ出力し、生成した数「R」を生成情報記憶領域に記憶する。

[0081] 「2×lenq」でないと判断する場合には、素数候補生成部142は、乱数生成部141より受け取った乱数「R1」に2を掛けて、その結果を「R1」として、再度、数「R」及び「N」を生成する。

「情報B」でないと判断する場合には、素数候補生成部142は、受け取った乱数「R

1」と読み出した発行識別子情報「IDI」とを用いて、数「R＝IDI×R1」を生成する。

素数候補生成部142は、回数読出命令を情報制御部140へ出力し、情報制御部140から、出力カウンタ136の値を受け取る。素数候補生成部142は、出力カウンタ136の値が「1」であるか否かを判断する。

[0082] 出力回数が「1」であると判断する場合には、素数候補生成部142は、情報制御部140の検証値記憶領域より第1検証値「c11」を読み出す。

出力回数が「1」でない、つまり「2」以上であると判断する場合には、素数候補生成部142は、情報制御部140の検証値記憶領域より第2検証値「c12」を読み出す。

なお、第1検証値「c11」を読み出した場合の動作と、第2検証値「c12」を読み出した場合の動作とは、同じであるため、以下においては、検証値「c」として説明する。

[0083] 素数候補生成部142は、読み出した素数「q」、発行識別子情報「IDI」、検証値「c」及び生成した数「R」とを用いて、数「N＝2×(R＋w)×q＋1」を生成する。このとき生成した数「N」が素数候補となる。

ここで、「w」は「2×w×q＋1＝c mod IDI、0≦w＜IDI」を満たす数である。「w」は、「w＝(c−1)×m mod IDI」を計算することにより求める。「m」は「(2×q)×m＝1 mod IDI」を満たす数である。上述したように、発行識別子情報「IDI」が奇数、すなわち、「GCD(IDI、2)＝1」であり、「IDI＜q」であるため、「m」は計算可能である。計算方法については、非特許文献5が詳しい。なお、以降において、第1検証値「c11」を用いた場合の「w」を「w1」と表記、及び第2検証値を用いた場合の「w」を「w2」と表記する。

[0084] 素数候補生成部142は、素数「q」のビットサイズ「lenq」を、情報制御部140の情報記憶領域より読み出し、生成した数「N」のビットサイズが「2×lenq」であるか否かを判断する。

「2×lenq」であると判断する場合には、素数候補生成部142は、生成した数「N」を第1素数判定部143へ出力し、生成した数「R」を生成情報記憶領域に記憶する。

[0085] 「2×lenq」でないと判断する場合には、素数候補生成部142は、乱数生成部141より受け取った乱数「R1」に2を掛けて、その結果を「R1」として、再度、数「R」及び「N」を生成する。

＜第1素数判定部143＞

第1素数判定部143は、数「N」を素数候補生成部142より受け取ると、受け取った数「N」を用いて、以下の式の成立を判定する。

[0086] $2^{(N-1)} = 1 \mod N \quad (eq1)$

ここで、2^(N−1)は、2のN−1乗を示している。

第1素数判定部143は、式(eq1)が成立していると判断する場合には、数「N」を第2素数判定部144へ出力する。

第1素数判定部143は、式(eq1)が成立していないと判断する場合には、乱数生成部141へ第2生成指示を出力する。

[0087] ＜第2素数判定部144＞

第2素数判定部144は、数「N」を第1素数判定部143より受け取ると、素数候補生成部142の生成情報記憶領域にて記憶されている数「R」を読み出す。

第2素数判定部144は、数「N」及び「R」とを用いて、以下の式の成立を判定する。

[0088] $2^{(2\times R)} \neq 1 \mod N \quad (eq2)$

第2素数判定部144は、式(eq2)が成立していると判断する場合には、数「N」を素数「N」として、情報制御部140を介して、繰返制御部132へ出力する。

第2素数判定部144は、式(eq2)が成立していないと判断する場合には、乱数生成部141へ第2生成指示を出力する。

[0089] (8)鍵判定部117

鍵判定部117は、素数生成部116より受け取った2つの素数「p1」及び「p2」を、記憶する素数記憶領域を有する。

鍵判定部117は、素数生成部116より素数「p1」及び「p2」を受け取ると、受け取った素数「p1」及び「p2」をそれぞれ素数記憶領域へ記憶する。

[0090] 鍵判定部117は、素数生成部116より判定開始命令を受け取ると、素数記憶領域にて記憶している2つの素数「p1」と「p2」とが一致するか否かを判断する。一致すると判断する場合には、記憶している素数「p2」を消去し、再生成命令を繰返制御部132へ出力する。

一致しないと判断する場合には、記憶している2つの素数「p1」及び「p2」を、秘密

鍵格納部111の素数格納領域へ書き込み、鍵生成開始命令を鍵生成部118へ出力する。

[0091] (9)鍵生成部118

鍵生成部118は、鍵判定部117より鍵生成命令を受け取ると、秘密鍵格納部111の素数格納領域にて記憶されている2つの素数「p1」及び「p2」を読み出し、読み出した素数「p1」と「p2」との積「n＝p1×p2」を計算する。

鍵生成部118は、乱数「e」を生成し、算出した「n」と、生成した乱数「e」とからなる組「PK＝(n、e)」を公開鍵として生成し、生成した公開鍵「PK」を公開鍵格納部112へ書き込む。ここで、乱数「e」は、従来と同様に、乱数「e」は、数「L」と互いに素であり、「1≦e≦L−1、GCD(e、L)＝1」を満たす。ここで、GCD(e、L)は、eとLの最大公約数を示し、数「L」は、「L＝LCM(p1−1、p2−1)」であり、LCM(p1−1、p2−1)は、「p1−1」と「p2−1」との最小公倍数を示す。

[0092] 鍵生成部118は、「e×d＝1 mod L」を満たす「d」を算出し、算出した「d」と、素数「p1」及び「p2」とからなる組「SK＝(p1、p2、d)」を秘密鍵として、秘密鍵格納部111の秘密鍵格納領域へ書き込む。鍵生成部118は、公開鍵証明書の要求処理を開始する要求開始命令を、情報取得部119へ出力する。

(10)情報取得部119

情報取得部119は、鍵生成部118から要求開始命令を受け取ると、識別子格納部110から発行識別子情報「IDI」と、公開鍵格納部112から公開鍵「PK」と、制御部114のサーバ識別子記憶領域130からサーバ識別子とを、それぞれ読み出す。情報取得部119は、読み出した発行識別子情報「IDI」と、公開鍵「PK」と、サーバ識別子と、公開鍵証明書の発行を依頼する証明書発行依頼情報とを送信部121を介して、証明書発行サーバ200へ送信する。

[0093] 情報取得部119は、制御部114から配布開始命令を受け取ると、秘密鍵格納部111にて記憶している秘密鍵「SK」と、証明書格納部113にて記憶している公開鍵証明書「Cert」と、制御部114の端末情報記憶領域にて記憶している端末識別子とを、それぞれ読み出し、読み出した秘密鍵「SK」及び公開鍵証明書「Cert」を、読み出した端末識別子に対応する端末装置300へ送信部121を介して送信する。

[0094] (11)受信部120

受信部120は、インターネットを介して、証明書発行サーバ200及び端末装置300より情報を受信し、受信した情報を、制御部114へ出力する。

(12)送信部121

送信部121は、情報取得部119より、発行識別子情報「IDI」と、公開鍵「PK」と、サーバ識別子と、証明書発行依頼情報とを受け取ると、受け取った各情報を証明書発行サーバ200へ送信する。

[0095] 送信部121は、情報取得部119より、秘密鍵「SK」及び公開鍵証明書「Cert」を受け取り、受け取った各情報を、端末装置300に送信する。

1．3 証明書発行サーバ200の構成

証明書発行サーバ200は、鍵発行サーバ100、101、及び102から証明書発行依頼情報を受け取ると、公開鍵証明書を発行し、発行した公開鍵証明書を発行依頼のあった鍵発行サーバへ送信する。

[0096] 証明書発行サーバ200は、図6にて示すように、秘密鍵格納部210、発行公開鍵格納部211、発行識別子情報格納部212、公開鍵証明書格納部213、発行公開鍵確認部214、公開鍵証明書生成部215、証明書取得部216、受信部217及び送信部218から構成されている。

証明書発行サーバ200は、具体的には、マイクロプロセッサ、ROM、RAM、ハードディスクユニット、ディスプレイユニット、キーボード、マウスなどから構成されるコンピュータシステムである。前記RAM又は前記ハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することにより、証明書発行サーバ200は、その機能を達成する。

[0097] なお、鍵発行サーバ100から証明書発行依頼情報を受け取った場合の動作と、他の鍵発行サーバから証明書発行依頼情報を受け取った場合の動作とは、同じであるため、以降の説明では、鍵発行サーバ100から送信された証明書発行依頼情報を用いて説明する。

(1)秘密鍵格納部210

秘密鍵格納部210は、証明書発行サーバ200のみが有する秘密鍵「SKCA」を予

め記憶している。

[0098] ここで、秘密鍵「SKCA」に対応する公開鍵「PKCA」は、端末装置400に配布されているものとする。

(2)発行公開鍵格納部211

発行公開鍵格納部211は、鍵発行サーバ100より受け取った公開鍵「PK」を記憶する領域を有している。

[0099] (3)発行識別子情報格納部212

発行識別子情報格納部212は、鍵発行サーバ100より受け取った発行識別子情報「IDI」を記憶する領域を有している。

(4)公開鍵証明書格納部213

公開鍵証明書格納部213は、発行した公開鍵証明書「Cert」を記憶する領域を有している。

[0100] (5)発行公開鍵確認部214

発行公開鍵確認部214は、図6に示すように、サーバ情報記憶領域220及び確認情報記憶領域221を有している。

サーバ情報記憶領域220は、公開鍵証明書の発行依頼のあった鍵発行サーバを識別するサーバ識別子を記憶する領域を有している。

[0101] 確認情報記憶領域221は、図7に示すように、検証値テーブルT200を有している。検証値テーブルT200は、サーバ識別子と、第1検証値と、第2検証値とからなる組を1以上記憶する領域を有している。サーバ識別子は、鍵発行サーバを識別する識別子であり、「SIDA」は、鍵発行サーバ100を示し、「SIDB」は、鍵発行サーバ101を示し、「SIDB」は、鍵発行サーバ102を示す。第1検証値及び第2検証値は、対応付けられたサーバ識別子にて示される鍵発行サーバに割り当てた検証値である。なお、以降では、鍵発行サーバ100のサーバ識別子を「SID」として説明する。

[0102] 発行公開鍵確認部214は、鍵発行サーバ100から受信部217を介して、発行識別子情報「IDI」と、公開鍵「PK」と、サーバ識別子と、証明書発行依頼情報とを受け取る。

発行公開鍵確認部214は、受け取ったサーバ識別子を、サーバ情報記憶領域22

0に書き込む。

[0103] 発行公開鍵確認部214は、受け取ったサーバ識別子を用いて、対応する第1検証値「c11」及び第2検証値「c12」を読み出す。

発行公開鍵確認部214は、受け取った公開鍵「PK」と発行識別子情報「IDI」とを用いて、公開鍵「PK」が、発行識別子情報「IDI」を用いて生成されたか否かを確認する。

[0104] ここで、確認方法について、説明する。公開鍵「PK」は、上述したように「PK＝(n、e)」である。発行公開鍵確認部214は、「n−(c11×c12)」を算出し、算出結果が、「IDI」で割り切れるか否かを検証する。これにより、公開鍵「PK」が、発行識別子情報「IDI」を用いて生成されたか否かを確認することができる。

発行公開鍵確認部214は、「n−(c11×c12)」が、「IDI」で割り切れると判断する場合には、公開鍵「PK」が、発行識別子情報「IDI」を用いて生成されたと判断し、「n−(c11×c12)」が、「IDI」で割り切れないと判断する場合には、公開鍵「PK」が、発行識別子情報「IDI」を用いて生成されていないと判断する。

[0105] 発行公開鍵確認部214は、公開鍵「PK」が、発行識別子情報「IDI」を用いて生成されたと判断する場合には、受け取った公開鍵「PK」を発行公開鍵格納部211へ、発行識別子情報を発行識別子情報格納部212へ、それぞれ書き込む。発行公開鍵確認部214は、公開鍵証明書の生成開始命令を公開鍵証明書生成部215へ出力する。

発行公開鍵確認部214は、公開鍵「PK」が、発行識別子情報「IDI」を用いて生成されていないと判断する場合には、処理を終了する。

[0106] (6)公開鍵証明書生成部215

公開鍵証明書生成部215は、発行公開鍵確認部214より、公開鍵証明書の生成開始命令を受け取ると、秘密鍵格納部210より秘密鍵「SKCA」を、発行公開鍵格納部211より公開鍵「PK」を、発行識別子情報格納部212より発行識別子情報「IDI」を、それぞれ読み出す。

[0107] 公開鍵証明書生成部215は、読み出した秘密鍵「SKCA」、公開鍵「PK」及び発行識別子情報「IDI」を用いて、公開鍵証明書「Cert」を生成する。生成する公開鍵

証明書「Cert」は、具体的には、「Cert＝n｜｜e｜｜IDI｜｜Sig(SKCA、n｜｜e｜｜IDI)」である。ここで、Sig(K、D)は、データ「D」に対して、秘密鍵「K」を用いたときの署名データである。記号「｜｜」は、ビットまたはバイトの連結である。

[0108] 公開鍵証明書生成部215は、生成した公開鍵証明書「Cert」を公開鍵証明書格納部213へ書き込み、公開鍵証明書「Cert」の送信開始命令を証明書取得部216へ出力する。

(7)証明書取得部216

証明書取得部216は、公開鍵証明書生成部215より、公開鍵証明書「Cert」の送信開始命令を受け取ると、公開鍵証明書格納部213から公開鍵証明書「Cert」を、サーバ情報記憶領域220からサーバ識別子を、それぞれ読み出し、読み出した公開鍵証明書「Cert」を、読み出したサーバ識別子に対応する鍵発行サーバ100へ送信部218を介して送信する。

[0109] (8)受信部217

受信部217は、鍵発行サーバ100より情報を受信し、受信した情報を、発行公開鍵確認部214へ出力する。

(9)送信部218

送信部218は、証明書取得部216より情報を受け取り、受け取った情報を鍵発行サーバ100へ送信する。

[0110] 1．4 端末装置300の構成

端末装置300は、図8にて示すように、秘密鍵格納部310、公開鍵証明書格納部311、制御部312、受付部313、無線部314、ベースバンド信号処理部315、スピーカー316、マイク317及び表示部318から構成されている。端末装置300の一例は、携帯電話機である。

[0111] 端末装置300は、具体的には、マイクロプロセッサ、ROM、RAM、ハードディスクユニット、ディスプレイユニット、キーボード、マウスなどから構成されるコンピュータシステムである。前記RAM又は前記ハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することにより、端末装置300は、その機能を達成する。

[0112] なお、端末装置301、・・・、302、303、・・、304、305、・・・、306は、端末装置300と同様の構成であるため、説明は省略する。

また、端末装置301、・・・、302から鍵発行依頼情報と、端末識別子とを、鍵発行サーバ100へ送信した場合、端末装置303、・・・、304から鍵発行依頼情報と、端末識別子とを、鍵発行サーバ101へ送信した場合、及び端末装置305、・・・、306から鍵発行依頼情報と、端末識別子とを、鍵発行サーバ102へ送信した場合の動作は、端末装置300から鍵発行依頼情報と、端末識別子とを、鍵発行サーバ100へ送信した場合の動作と同じであるため、以降の説明では、鍵発行依頼情報と、端末識別子とを、鍵発行サーバ100へ送信した場合の動作について説明する。

[0113] (1)秘密鍵格納部310

秘密鍵格納部310は、鍵発行依頼情報を送信した鍵発行サーバ、ここでは、鍵発行サーバ100にて発行された秘密鍵「SK＝(p1、p2、d)」を記憶する領域を有している。

(2)公開鍵証明書格納部311

公開鍵証明書格納部311は、鍵発行サーバ100にて発行された秘密鍵に対応する公開鍵の公開鍵証明書「Cert」を記憶する領域を有している。

[0114] (3)制御部312

制御部312は、図8にて示すように、端末識別子記憶領域320を有している。

制御部312は、暗号化された電子メールを記憶するメール記憶領域をも有している。

端末識別子記憶領域320は、当該装置を識別する端末識別子「TID」を予め記憶している。

[0115] 制御部312は、受付部313より鍵発行要求の指示を受け付けると、端末識別子記憶領域320から端末識別子「TID」を読み出す。

制御部312は、鍵発行依頼情報と、読み出した端末識別子「TID」とを、鍵発行サーバ100へ、ベースバンド信号処理部315及び無線部314を介して送信する。

制御部312は、鍵発行サーバ100より、無線部314及びベースバンド信号処理部315を介して、秘密鍵「SK」及び公開鍵証明書「Cert」を受け取ると、受け取った秘密

鍵「SK」を秘密鍵格納部310へ、公開鍵証明書「Cert」を公開鍵証明書格納部311へ、それぞれ書き込む。

[0116] 制御部312は、端末装置400より、無線部314及びベースバンド信号処理部315を介して、暗号化された電子メールを受け取ると、受け取った暗号化された電子メールをメール記憶領域へ書き込む。

制御部312は、受付部313より、暗号化された電子メールの表示命令を受け取ると、秘密鍵格納部310より秘密鍵「SK」を、メール記憶領域より暗号化された電子メールを、それぞれ読み出し、読み出した秘密鍵「SK」を用いて、暗号化された電子メールを復号し、復号された電子メール(以下、単に「電子メール」という。)を表示部318へ出力する。

[0117] (4)受付部313

受付部313は、ユーザの操作により、鍵発行要求の指示を受け付けると、受け付けた指示を制御部312へ出力する。

受付部313は、ユーザの操作により、暗号化された電子メールの表示の指示を受け付けると、表示命令を制御部312へ出力する。

[0118] (5)無線部314

無線部314は、アンテナ319を備えており、無線信号の送受信を行う。

(6)ベースバンド信号処理部315

ベースバンド信号処理部315は、無線部314より受け取った信号をスピーカー316へ出力するための信号処理や、マイク317より受け取った音声を無線部314へ出力するための信号処理を行う。

[0119] ベースバンド信号処理部315は、制御部312から鍵発行依頼情報及び端末識別子を受け取ると、受け取ったから鍵発行依頼情報及び端末識別子を、無線部314を介して鍵発行サーバ100へ送信する。

ベースバンド信号処理部315は、鍵発行サーバ100から秘密鍵及び公開鍵証明書とを、無線部314を介して受け取ると、受け取った秘密鍵及び公開鍵証明書を制御部312へ出力する。

[0120] ベースバンド信号処理部315は、鍵発行サーバ100から秘密鍵及び公開鍵証明

書とを、無線部314を介して受け取ると、受け取った秘密鍵及び公開鍵証明書を制御部312へ出力する。

ベースバンド信号処理部315は、端末装置400から暗号化された電子メールを、無線部314を介して受け取ると、受け取った暗号化された電子メールを制御部312へ出力する。

[0121] (7)スピーカー316

スピーカー316は、ベースバンド信号処理部315にて処理された信号を音声として出力する。

(8)マイク317

マイク317は、使用者の音声を受け付け、受け付けた音声をベースバンド信号処理部315へ出力する。

[0122] (9)表示部318

表示部318は、制御部312より受け取った電子メールを表示する。

1．5 鍵発行システム1の動作

ここでは、鍵発行システム1の動作について説明する。

(1)鍵発行システム1の動作概要

鍵発行システム1の動作概要を図9に示す流れ図を用いて、説明する。

[0123] 以下では、鍵発行サーバ100が端末装置300に鍵を発行するときの動作概要を示す。

端末装置300は、まず、鍵依頼処理にて、鍵発行依頼情報及び端末識別子「TID」を鍵発行サーバ100へ送信する(ステップS5)。

鍵発行サーバ100は、端末装置300より鍵発行依頼情報及び端末識別子「TID」を受信すると、鍵発行処理にて、発行識別子情報「IDI」、秘密鍵「SK＝(p1、p2、d)」及び公開鍵「PK＝(n、e)」を生成する。鍵発行サーバ100は、生成した発行識別子情報「IDI」及び公開鍵「PK」と、証明書発行依頼情報と、サーバ識別子「SID」とを、証明書発行サーバ200へ送信する(ステップS10)。

[0124] 証明書発行サーバ200は、発行識別子情報「IDI」及び公開鍵「PK」と、証明書発行依頼情報と、サーバ識別子「SID」とを受信すると、証明書発行処理にて、公開鍵「

PK」に対応する秘密鍵「SK」に含まれる素数「p1」、「p2」が発行識別子情報「IDI」を用いて生成されているかを判定し、判定結果が肯定的な場合に、公開鍵「PK」に対する公開鍵証明書「Cert」を生成する。証明書発行サーバ200は、生成した公開鍵証明書「Cert」を鍵発行サーバ100へ送信する(ステップS15)。

[0125] 鍵発行サーバ100は、鍵発行処理にて、証明書発行サーバ200から公開鍵証明書「Cert」を受信すると、秘密鍵「SK=(p1、p2、d)」と公開鍵証明書「Cert」を端末装置300へ送信する(ステップS20)。

端末装置300は、鍵依頼処理にて、鍵発行サーバ100から秘密鍵「SK」と公開鍵証明書「Cert」とを受信すると、受信した秘密鍵「SK」、公開鍵証明書「Cert」を格納し、システムを終了する。

[0126] (2)鍵依頼処理

ここでは、図9に示す鍵依頼処理の動作について、図10に示す流れ図を用いて、説明する。なお、ここでは、端末装置300及び鍵発行サーバ100を用いて、鍵依頼処理の動作を説明する。

端末装置300の受付部313は、ユーザの操作により、鍵発行要求の指示を受け付ける(ステップS100)。

[0127] 端末装置300の制御部312は、端末識別子記憶領域320から端末識別子「TID」を取得する(ステップS105)。

端末装置300の制御部312は、鍵発行依頼情報と、取得した端末識別子「TID」とを、鍵発行サーバ100へ、ベースバンド信号処理部315及び無線部314を介して送信する(ステップS110)。

[0128] 端末装置300の制御部312は、鍵発行サーバ100より、無線部314及びベースバンド信号処理部315を介して、秘密鍵「SK」及び公開鍵証明書「Cert」を受け取る(ステップS115)。

制御部312は、受け取った秘密鍵「SK」を秘密鍵格納部310へ書き込み(ステップS120)、公開鍵証明書「Cert」を公開鍵証明書格納部311へ書き込む(ステップS125)。

[0129] (3)鍵発行処理

ここでは、図9に示す鍵発行処理の動作について、図11、図12、図13及び図13に示す流れ図を用いて、説明する。

鍵発行サーバ100の制御部114は、端末装置300から受信部120を介して、鍵発行依頼情報と、端末装置300の端末識別子「TID」とを受け取ると(ステップS200)、受け取った端末識別子「TID」を端末情報記憶領域131へ書き込み、発行識別子情報の生成命令と、受け取った端末識別子「TID」とを識別子生成部115へ出力する(ステップS205)。

[0130] 識別子生成部115は、制御部114から発行識別子情報の生成命令と、端末識別子「TID」とを受け取ると、サーバ識別子記憶領域にて記憶されているサーバ識別子「SID」を取得する。識別子生成部115は、取得したサーバ識別子「SID」と、受け取った端末識別子「TID」と数「1」とから、発行識別子情報「IDI」を生成し、生成した発行識別子情報「IDI」を識別子格納部110へ書き込み、素数の生成命令を素数生成部116へ出力する(ステップS210)。

[0131] 繰返制御部132は、識別子生成部115から素数の生成開始命令を受け取ると、繰返カウンタ135及び出力カウンタ136を、それぞれ「1」に設定する(ステップS215)。

繰返制御部132は、繰返カウンタ135の値が、1であるか否かを判断する(ステップS220)。

[0132] 1であると判断する場合には(ステップS220における「YES」)、繰返制御部132は、初期値記憶領域より素数とそのビットサイズを読み出し(ステップS225)、1でないと判断する場合には(ステップS220における「NO」)、一時記憶領域よりビットサイズ「8×(2^(n−1))」と、その素数、つまり前回生成した素数とそのビットサイズとを読み出す(ステップS230)。つまり、繰返制御部132は、繰返カウンタ135の値が、1でないと判断する場合には、一時記憶領域より、前回生成した素数とそのビットサイズとを読み出す。ここで、「n」は、繰返カウンタの値である。

[0133] 繰返カウンタ135の値に対応する制御情報を制御情報テーブルT100より読み出し(ステップS235)、読み出した制御情報が、「情報C」であるか否かを判断する(ステップS240)。

「情報C」であると判断する場合には(ステップS240における「YES」)、繰返制御部

132は、読み出した素数及びそのビットサイズと、制御情報とからなる第1情報を生成し、生成した第1情報を、素数情報生成部133へ出力する(ステップS245)。

[0134] 「情報C」でないと判断する場合には(ステップS240における「NO」)、繰返制御部132は、識別子格納部110より発行識別子情報「IDI」を取得し、取得した発行識別子情報「IDI」のビットサイズ「lenIDI」を算出し、読み出した素数及びそのビットサイズと、制御情報と、発行識別子情報「IDI」及びそのビットサイズ「lenIDI」とからなる第2情報を生成し、生成した第2情報を、素数情報生成部133へ出力する(ステップS250)。

[0135] 素数情報生成部133は、素数生成処理により素数を生成し、生成した素数を繰返制御部132へ出力する(ステップS255)。

繰返制御部132は、素数情報生成部133から、素数を受け取ると、繰返カウンタ135の値に「1」を加算し(ステップS260)、加算結果が、7であるか否かを判断する(ステップS265)。

[0136] 加算結果が7でないと判断する場合には(ステップS265における「NO」)、繰返制御部132は、受け取った素数のビットサイズを算出し(ステップS270)、受け取った素数と、算出したビットサイズとを一時的に記憶し(ステップS275)、ステップS220へ戻る。

加算結果が7であると判断する場合には(ステップS265における「YES」)、繰返制御部132は、出力カウンタ136の値が、1であるか否かを判断する(ステップS280)。

[0137] 1であると判断する場合には(ステップS280における「YES」)、繰返制御部132は、受け取った素数を素数「p1」として、鍵判定部117へ出力し(ステップS285)、出力カウンタ136の値に「1」を加算し(ステップS290)、繰返カウンタ135の値に「1」を設定し(ステップS295)、ステップS220へ戻る。

1でない、つまり2以上であると判断する場合には(ステップSNOにおける「NO」)、繰返制御部132は、受け取った素数を素数「p2」として、素数「p2」と判定開始命令を鍵判定部117へ出力する(ステップS300)。

[0138] 鍵判定部117は、ステップS285にて繰返制御部132より素数「p1」を受け取ると、受け取った素数「p1」を素数記憶領域へ記憶する。鍵判定部117は、ステップS300

にて繰返制御部132より「p2」及び判定開始命令とを受け取ると、受け取った素数「p2」を素数記憶領域へ記憶する。鍵判定部117は、素数記憶領域にて記憶している2つの素数「p1」と「p2」とが一致するか否かを判断する(ステップS305)。一致すると判断する場合には、記憶している素数「p2」を消去し、再生成命令を繰返制御部132へ出力し(ステップS305における「YES」)、繰返制御部132は、鍵判定部117より素数を再度生成する旨の再生成命令を受け取ると、上述したステップS290及びステップS295を行い、ステップS220へ戻る。

[0139] 一致しないと判断する場合には、記憶している2つの素数「p1」及び「p2」を、秘密鍵格納部111の素数格納領域へ書き込み、鍵生成開始命令を鍵生成部118へ出力し(ステップS305における「NO」)、鍵生成部118は、鍵判定部117より鍵生成命令を受け取ると、秘密鍵格納部111の素数格納領域にて記憶されている2つの素数「p1」及び「p2」を読み出し、読み出した素数「p1」と「p2」との積「n=p1×p2」を計算する(ステップS310)。

[0140] 鍵生成部118は、乱数「e」を生成し(ステップS315)、算出した「n」と、生成した乱数「e」とからなる組「PK=(n、e)」を公開鍵として生成し、生成した公開鍵「PK」を公開鍵格納部112へ書き込む(ステップS320)。ここで、乱数「e」は、従来と同様に、乱数「e」は、数「L」と互いに素であり、「1≦e≦L−1、GCD(e、L)=1」を満たす。数「L」は、「L=LCM(p1−1、p2−1)」である。

[0141] 鍵生成部118は、「e×d=1 mod L」を満たす「d」を算出し(ステップS325)、算出した「d」と、素数「p1」及び「p2」とからなる組「SK=(p1、p2、d)」を秘密鍵として、秘密鍵格納部111の秘密鍵格納領域へ書き込み、要求開始命令を、情報取得部119へ出力する(ステップS330)。

情報取得部119は、鍵生成部118から要求開始命令を受け取ると、識別子格納部110から発行識別子情報「IDI」と、公開鍵格納部112から公開鍵「PK」と、制御部114のサーバ識別子記憶領域130からサーバ識別子とを、それぞれ読み出す(ステップS335)。情報取得部119は、読み出した発行識別子情報「IDI」と、公開鍵「PK」と、サーバ識別子と、公開鍵証明書の発行を依頼する証明書発行依頼情報とを送信部121を介して、証明書発行サーバ200へ送信する(ステップS340)。

[0142] 制御部114は、証明書発行サーバ200から受信部120を介して、公開鍵証明書「Cert」を受け取ると、受け取った公開鍵証明書「Cert」を証明書格納部113へ書き込み、配布開始命令を情報取得部119へ出力する(ステップS345)。

情報取得部119は、制御部114から配布開始命令を受け取ると、秘密鍵格納部111にて記憶している秘密鍵「SK」と、証明書格納部113にて記憶している公開鍵証明書「Cert」と、制御部114の端末情報記憶領域にて記憶している端末識別子とを、それぞれ読み出し(ステップS350)、読み出した秘密鍵「SK」及び公開鍵証明書「Cert」を、読み出した端末識別子に対応する端末装置300へ送信部121を介して送信する(ステップS355)。

[0143] (4)素数生成処理

ここでは、図12に示す素数生成処理の動作について、図15に示す流れ図を用いて、説明する。

情報制御部140は、繰返制御部132から、素数「q」と、素数のビットサイズ「lenq」と、制御情報とからなる第1情報及び素数「q」と、素数のビットサイズ「lenq」と、制御情報と、発行識別子情報「IDI」と、そのビットサイズ「lenIDI」とからなる第2情報の何れかを受け取ると、受け取った情報を情報記憶領域へ書き込み、乱数の生成の指示を示す第1生成指示を、乱数生成部141へ出力する(ステップS400)。

[0144] 乱数生成部141は、乱数の生成の指示を示す第1生成指示を、情報制御部140から受け取ると、情報制御部140の情報記憶領域にて記憶されている制御情報を読み出し(ステップS405)、読み出した制御情報が「情報C」であるか否かを判断する(ステップS410)。

「情報C」であると判断する場合には(ステップS410における「YES」)、乱数生成部141は、情報制御部140の情報記憶領域にて記憶されている「lenq」を読み出し(ステップS415)、(lenq−1)ビットからなる乱数「R1」を生成し、生成した乱数「R1」と読み出した制御情報とを素数候補生成部142へ出力する(ステップS420)。ここで、乱数「R1」の最上位ビットは1とする。乱数生成方法は、非特許文献2が詳しい。

[0145] 「情報C」でないと判断する場合には(ステップS410における「NO」)、乱数生成部141は、情報制御部140の情報記憶領域にて記憶されている「lenq」及び「lenIDI」

を読み出し(ステップS425)、(lenq−lenIDI−1)ビットからなる乱数「R1」を生成し、生成した乱数「R1」と読み出した制御情報とを素数候補生成部142へ出力する(ステップS430)。ここで、乱数「R1」の最上位ビットは1とする。

[0146] 素数候補生成部142は、素数候補生成処理により、乱数「R」と、素数候補である数「N」とを生成し、生成した乱数「R」を生成情報記憶領域に記憶し、生成した数「N」を第1素数判定部143へ出力する(ステップS435)。

第1素数判定部143は、数「N」を素数候補生成部142より受け取ると、受け取った数「N」を用いて、上述した式(eq1)が成立するか否かを判断する(ステップS440)。

[0147] 第1素数判定部143は、式(eq1)が成立していると判断する場合には、数「N」を第2素数判定部144へ出力し(ステップS440における「YES」)、第2素数判定部144は、数「N」を第1素数判定部143より受け取ると、素数候補生成部142の生成情報記憶領域にて記憶されている数「R」を読み出し、上述した式(eq2)が成立するか否かを判断する(ステップS445)。

[0148] 第2素数判定部144は、式(eq2)が成立していると判断する場合には(ステップS445における「YES」)、数「N」を素数「N」として、情報制御部140を介して、繰返制御部132へ出力する(ステップS450)。

第1素数判定部143は、式(eq1)が成立していないと判断する場合には、乱数生成部141へ第2生成指示を出力(ステップS440における「NO」)、第2素数判定部144は、式(eq2)が成立していないと判断する場合には、乱数生成部141へ第2生成指示を出力し(ステップS445における「NO」)、乱数生成部141は、第1素数判定部143及び第2素数判定部144の何れかから、再度乱数を生成する旨の第2生成指示を受け付けると、ステップS405に戻る。

[0149] (5)素数候補生成処理

ここでは、図15に示す素数候補生成処理の動作について、図16及び図17に示す流れ図を用いて、説明する。

素数候補生成部142は、乱数生成部141より、乱数「R1」と制御情報とを受け取ると(ステップS500)、受け取った制御情報が「情報C」であるか否かの判断をする(ステップS505)。

[0150] 「情報C」であると判断する場合には(ステップS505における「YES」)、素数候補生成部142は、情報制御部140の情報記憶領域より素数「q」を読み出す(ステップS510)。素数候補生成部142は、読み出した素数「q」と乱数生成部141より受け取った乱数「R1」とを用いて、数「N＝2×R1×q＋1」を生成する(ステップS515)。素数候補生成部142は、生成した数「N」のビットサイズ「lenN」が「lenq」と一致するか否かを判断し(ステップS520)、一致すると判断する場合には(ステップS520における「YES」)、素数候補生成部142は、生成した数「N」を第1素数判定部143へ出力し、受け取った乱数「R1」を、「R」として生成情報記憶領域に記憶する(ステップS595)。

[0151] 一致しないと判断する場合には(ステップS520における「NO」)、素数候補生成部142は、乱数生成部141より受け取った乱数「R1」に2を掛けて、その結果を「R1」とし(ステップS525)、ステップS515に戻る。

制御情報が「情報C」でないと判断する場合には(ステップS505における「NO」)、素数候補生成部142は、情報制御部140の情報記憶領域より素数「q」及び発行識別子情報「IDI」を読み出す(ステップS530)。素数候補生成部142は、制御情報が「情報B」であるか否かを判断する(ステップS535)。

[0152] 「情報B」であると判断する場合には(ステップS535における「YES」)、素数候補生成部142は、受け取った乱数「R1」と読み出した発行識別子情報「IDI」とから、結合値「IDI｜｜R1」を生成し、生成した結合値「IDI｜｜R1」と関数記憶領域にて記憶している関数「f」とを用いて、数「R＝f(IDI｜｜R1)」を生成する(ステップS540)。素数候補生成部142は、生成した数「R」と読み出した素数「q」とを用いて、数「N＝2×R×q＋1」を生成する(ステップS545)。

[0153] 素数候補生成部142は、生成した数「N」のビットサイズ「lenN」が「2×lenq」であるか否かを判断する(ステップS550)。

「2×lenq」であると判断する場合には(ステップS550における「YES」)、素数候補生成部142は、生成した数「N」を第1素数判定部143へ出力し、生成した数「R」を生成情報記憶領域に記憶する(ステップS595)。

[0154] 「2×lenq」でないと判断する場合には(ステップS550における「NO」)、素数候補生成部142は、乱数生成部141より受け取った乱数「R1」に2を掛けて、その結果を「

R1」とし(ステップS555)、ステップS540へ戻る。

「情報B」でないと判断する場合には(ステップS535における「NO」)、素数候補生成部142は、受け取った乱数「R1」と読み出した発行識別子情報「IDI」とを用いて、数「R＝IDI×R1」を生成する(ステップS560)。素数候補生成部142は、回数読出命令を情報制御部140へ出力し、情報制御部140から、出力カウンタ136の値を受け取る。素数候補生成部142は、受け取った値が「1」であるか否かを判断する(ステップS565)。

[0155] 出力回数が「1」であると判断する場合には(ステップS565における「YES」)、素数候補生成部142は、情報制御部140の検証値記憶領域より第1検証値「c11」を読み出す(ステップS570)。素数候補生成部142は、読み出した素数「q」、発行識別子情報「IDI」、検証値「c11」及び生成した数「R」とを用いて、数「N＝2×(R＋w1)×q＋1」を生成する(ステップS575)。ここで、「w1」は「2×w1×q＋1＝c11 mod IDI、0≦w1＜IDI」を満たす数である。

[0156] 出力回数が「1」でない、つまり「2」以上であると判断する場合には(ステップS565における「NO」)、素数候補生成部142は、情報制御部140の検証値記憶領域より第2検証値「c12」を読み出す(ステップS580)。素数候補生成部142は、読み出した素数「q」、発行識別子情報「IDI」、検証値「c12」及び生成した数「R」とを用いて、数「N＝2×(R＋w2)×q＋1」を生成する(ステップS585)。ここで、「w2」は「2×w2×q＋1＝c12 mod IDI、0≦w2＜IDI」を満たす数である。

[0157] 素数候補生成部142は、素数「q」のビットサイズ「lenq」を、情報制御部140の情報記憶領域より読み出し、生成した数「N」のビットサイズが「2×lenq」であるか否かを判断する(ステップS590)。

「2×lenq」であると判断する場合には(ステップS590における「YES」)、素数候補生成部142は、生成した数「N」を第1素数判定部143へ出力し、生成した数「R」を生成情報記憶領域に記憶する(ステップS595)。

[0158] 「2×lenq」でないと判断する場合には(ステップS590における「NO」)、素数候補生成部142は、乱数生成部141より受け取った乱数「R1」に2を掛けて、その結果を「R1」とし(ステップS600)、ステップS560に戻る。

(6)証明書発行処理

ここでは、図9に示す証明書発行処理の動作について、図18に示す流れ図を用いて、説明する。

[0159] 証明書発行サーバ200の発行公開鍵確認部214は、鍵発行サーバ100から受信部217を介して、発行識別子情報「IDI」と、公開鍵「PK」と、サーバ識別子と、証明書発行依頼情報とを受け取る(ステップS650)。

発行公開鍵確認部214は、受け取ったサーバ識別子を、サーバ情報記憶領域220に書き込む(ステップS655)。

[0160] 発行公開鍵確認部214は、受け取ったサーバ識別子を用いて、対応する第1検証値「c11」及び第2検証値「c12」を読み出す(ステップS660)。

発行公開鍵確認部214は、読み出した第1検証値「c11」及び第2検証値「c12」と、受け取った公開鍵「PK」と、発行識別子情報「IDI」とを用いて、公開鍵「PK」が、発行識別子情報「IDI」を用いて生成されたか否かを確認する(ステップS660)。

[0161] 発行公開鍵確認部214は、「n−(c11×c12)」が、「IDI」で割り切れると判断する場合、つまり公開鍵「PK」が、発行識別子情報「IDI」を用いて生成されたと判断する場合には(ステップS660における「YES」)、発行公開鍵確認部214は、受け取った公開鍵「PK」を発行公開鍵格納部211へ、発行識別子情報を発行識別子情報格納部212へ、それぞれ書き込み、発行公開鍵確認部214は、公開鍵証明書の生成開始命令を公開鍵証明書生成部215へ出力する(ステップS665)。

[0162] 発行公開鍵確認部214は、公開鍵「PK」が、発行識別子情報「IDI」を用いて生成されていないと判断する場合には(ステップS660における「YES」)、処理を終了する。

公開鍵証明書生成部215は、発行公開鍵確認部214より、公開鍵証明書の生成開始命令を受け取ると、秘密鍵格納部210より秘密鍵「SKCA」を、発行公開鍵格納部211より公開鍵「PK」を、発行識別子情報格納部212より発行識別子情報「IDI」を、それぞれ読み出す(ステップS670)。

[0163] 公開鍵証明書生成部215は、読み出した秘密鍵「SKCA」、公開鍵「PK」及び発行識別子情報「IDI」を用いて、公開鍵証明書「Cert」を生成し、生成した公開鍵証

明書「Cert」を公開鍵証明書格納部213へ書き込み、公開鍵証明書「Cert」の送信開始命令を証明書取得部216へ出力する(ステップS675)。

証明書取得部216は、公開鍵証明書生成部215より、公開鍵証明書「Cert」の送信開始命令を受け取ると、公開鍵証明書格納部213から公開鍵証明書「Cert」を、サーバ情報記憶領域220からサーバ識別子を、それぞれ読み出し、読み出した公開鍵証明書「Cert」を、読み出したサーバ識別子に対応する鍵発行サーバ100へ送信部218を介して送信する(ステップS680)。

[0164] 1.6 素数情報生成部133の動作検証

素数情報生成部133の第1素数判定部143及び、第2素数判定部144は、Pocklington判定である。Pocklington判定は、非特許文献1の144ページ及び非特許文献4が詳しい。以下に、簡単に説明する。

Pocklington判定によると、「N=2×R×q+1」の「q」が素数であり

$2^{(N-1)} = 1 \mod N$

$2^{(2R)} \neq 1 \mod N$

の両方が成り立つ場合、数「N」は素数となり、素数情報生成部133は、数「N」を素数として出力することができる。

[0165] また、乱数「R1」のビットサイズが(lenq−lenIDI−1)であるので、数「R」のビットサイズが(lenq−1)になり、ほとんどの数「N」のビットサイズが(2×lenq)になる。ここで、素数「q」や発行識別子情報「IDI」などの値によっては、ビットサイズが(2×lenq−1)となる場合がある。その場合は、素数候補生成部142は、上述したように、R1に2を掛けて、それを新たにR1とすることにより、生成する数「N」のビットサイズを(2×lenq)になるように設定することができる。

[0166] 1.7 第1の実施の形態の効果

(1)生成される鍵の一意性

ここでは、鍵発行サーバ100にて生成される鍵、つまり素数の一意性について説明する。

ここで、以下の命題を証明する。

[0167] (命題)発行識別子情報IDIが異なれば、出力される素数「N」が異なる。

まず、以下の補題を証明し、その補題を用いて、上記の命題を証明する。

(補題)二つの素数「p1＝2×q1×R1＋1」及び「p2＝2×q2×R2＋1」に対し、p1＝p2であれば、q1＝q2かつR1＝R2となる。

(証明)p1＝p2の場合、素数「q1」及び「q2」のビットサイズは、それぞれ256ビットであり、数「R1」及び「R2」のビットサイズは、それぞれ255ビットであるため、q1＝q2となるのは明らか。また、q1＝q2より、R1＝R2も成り立つ(証明終)。

[0168] 上記補題より、p1＝p2であれば、R1＝R2が成り立つ。R1＝f(IDI1｜｜R11)、R2＝f(IDI2｜｜R22)とおくと、R1＝R2であり、fは単射であるため、IDI1＝IDI2が成り立つ。したがって、この対偶を取ることにより、上記の命題が成り立つ。 以上より、IDIが異なれば必ず素数が異なる。したがって、鍵発行サーバ100に与えるIDIを毎回変えることで、毎回異なる素数を生成することができる。これにより、生成される素数は、一意性が保たれる。

[0169] したがって、複数回生成した素数が一致しないことを比較することなく、証明できる。

(2)生成された鍵の正当性

鍵発行サーバ100にて生成された素数「p1」に対して、「p1−c11」は必ず発行識別子情報「IDI」で割り切れる。

なぜなら、「p1−c11＝2×q×(R＋w1)＋1−c11＝2×q×(IDI×R1＋w1)＋1−c11＝2×q×IDI×R1＋2×q×w1＋1−c11」であり、項「2×q×IDI×R」は、「IDI」で割り切れることが分かる。また、上述したように、「2×q×w1＋1＝c11 mod IDI」が成り立っているため、残りの項「2×q×w1＋1−c11」も「IDI」で割り切れる。つまり、鍵発行サーバ100にて生成された素数「p1」に対して、「p1−c11」は必ず発行識別子情報「IDI」で割り切れる。したがって、生成された素数「p1」に対し、「p1−c11」が発行識別子情報「IDI」で割り切れるか否かで、鍵発行サーバ100を用いて素数が生成されたかを確認することができる。

[0170] また、上記と同様の理由により、素数「p1」に対して、「p2−c12」は必ず発行識別子情報「IDI」で割り切れる。

したがって、「n−c11×c12」は「IDI」で割り切れるため、証明書発行サーバ200は、「n−c11×c12」が「IDI」で割り切れることを確認することで、素数「p1」、「p2」が正

しく発行識別子情報「IDI」を用いて生成しているかを確認することができる。

[0171] なぜなら、秘密鍵である素数「p1」、「p2」はそれぞれ、素数「q1」、「q2」、乱数「R1 1」、「R12」、発行識別子情報「IDI」に対して、「p1＝2×q1×(IDI×R11＋w1)＋1＝c11 mod IDI」、「p2＝2×q2×(IDI×R12＋w1)＋1＝c12 mod IDI」を満たすため、

$$n=p1\times p2=(2\times q1\times IDI\times R11+1)\times(2\times q2\times IDI\times R12+1)$$
$$=c11\times c12 \bmod IDI$$

となる。そのため、証明書発行サーバ200は、「n−c11×c12」が「IDI」で割り切れるか否かを確認することにより、鍵発行サーバが正しく発行識別子情報IDIを用いて生成しているかを確認することができる。

[0172] なお、「IDI」のビットサイズが「lenIDI」であり、「R1」のビットサイズが(lenq−lenIDI −1)であるため、ほとんどの「N1＝2×q×(IDI×R1＋w)＋1」のビットサイズは、2 ×lenq1となる。ここで、「q1」や「IDI」などの値によっては、ビットサイズが(2×lenq− 1)となる場合がある。その場合は、素数候補生成部142で、「R1」に2を掛けて、それを新たに「R1」とみなすことにより、「N1」のビットサイズを「2×lenq1」になるように設定することができる。

[0173] さらに、鍵発行システム1は、端末がその端末がもつ秘密鍵を用いて、不正を働いたとき、以下の確認方法により、秘密鍵より不正を働いた端末の情報を得ることができる。不正を働いた端末の秘密鍵「p1」、「p2」が判明したとする。また、不正の追跡者、例えば証明書発行サーバ200の管理者は、発行識別子情報と端末の対応表と持っているとする。「p1−c11」、「p2−c12」は共に発行識別子情報「IDI」で割り切れる。そのため、GCD(p1−c11、p2−c12)は発行識別子情報で割り切れる。したがって、GCD(p1−c11、p2−c12)の素因数を調べることにより、不正の追跡者は、取りうる発行識別子情報を限定でき、発行識別子情報を知る、すなわち、端末を特定するための助けとなる。

[0174] 1．10 素数生成の変形例1

上記実施の形態では、第1検証値及び第2検証値の2つの検証値を用いたが、ここでは、1つの検証値を用いた場合の素数の生成について、説明する。

上記実施の形態と異なる点は、鍵発行サーバにおける素数情報生成部と、証明書発行サーバにおける発行公開鍵確認部とが異なる。以下に、本変形例における素数情報生成部133A、及び発行公開鍵確認部214Aについて説明する。なお、他の構成要素については、第1の実施の形態にて示した構成要素を用いる。

[0175] (1)素数情報生成部133A

素数情報生成部133Aは、図19に示すように、情報制御部140A、乱数生成部141A、素数候補生成部142A、第1素数判定部143A及び第2素数判定部144Aから構成されている。

素数情報生成部133Aは、繰返制御部132から受け取った素数のビットサイズが2倍のビットサイズからなる素数を生成する。

[0176] なお、以下の説明において、繰返制御部132から受け取る素数を素数「q」、そのビットサイズを「lenq」として、各構成要素について説明する。

＜情報制御部140A＞

情報制御部140Aは、第1情報及び第2情報を記憶するための情報記憶領域を有している。

[0177] 情報制御部140Aは、証明書発行サーバ200により割り当てられ、且つ制御情報「情報A」に基づいて素数を生成する際に用いる検証値「c1」を予め記憶している検証値記憶領域を有している。

情報制御部140Aは、繰返制御部132から、素数「q」と、素数のビットサイズ「lenq」と、制御情報とからなる第1情報を受け取ると、受け取った第1情報を情報記憶領域へ書き込む。つまり、素数「q」と、素数のビットサイズ「lenq」と、制御情報(この場合、「情報C」)とを書き込む。

[0178] 情報制御部140Aは、繰返制御部132から、素数「q」と、素数のビットサイズ「lenq」と、制御情報と、発行識別子情報「IDI」と、そのビットサイズ「lenIDI」とからなる第2情報を受け取ると、受け取った第2情報を情報記憶領域へ書き込む。つまり、素数「q」と、素数のビットサイズ「lenq」と、制御情報、発行識別子情報「IDI」と、そのビットサイズ「lenIDI」とを書き込む。

[0179] 情報制御部140Aは、受け取った情報の書き込み後、乱数の生成の指示を示す第

1生成指示を、乱数生成部141Aへ出力する。

情報制御部140Aは、第2素数判定部144Aより、素数を受け取ると、受け取った素数を繰返制御部132へ出力する。

＜乱数生成部141A＞

乱数生成部141Aは、第1の実施の形態にて示す乱数生成部141Aと同様であるため、説明は省略する。

[0180] ＜素数候補生成部142A＞

素数候補生成部142Aは、生成された情報を記憶する生成情報記憶領域と、単射である関数「f」を予め記憶している関数記憶領域とを有している。ここで、関数「f」は、例えば、f(X||Y)＝Enc(K、X||Y)である。Enc(K、X||Y)は鍵Xを用いたときの(X||Y)の共通鍵暗号による暗号文である。共通鍵暗号の暗号化関数は一般的に全単射である。また、記号「||」はビットまたはバイト連結である。暗号化関数「Enc(K、X||Y)」の一例は、「Enc(K、X||Y)＝K XOR X||Y」である。なお、共通暗号の一例は、DESであり、DESを用いる場合には、鍵長は128ビットとなる。

[0181] 素数候補生成部142Aは、乱数生成部141Aより、乱数「R1」と制御情報とを受け取ると、受け取った制御情報が「情報C」であるか否かの判断をする。

「情報C」であると判断する場合には、素数候補生成部142Aは、情報制御部140Aの情報記憶領域より素数「q」を読み出す。素数候補生成部142Aは、読み出した素数「q」と乱数生成部141Aより受け取った乱数「R1」とを用いて、数「N＝2×R1×q＋1」を生成する。素数候補生成部142Aは、生成した数「N」のビットサイズ「lenN」が「lenq」と一致するか否かを判断し、一致すると判断する場合には、素数候補生成部142Aは、生成した数「N」を第1素数判定部143Aへ出力し、受け取った乱数「R1」を、「R」として生成情報記憶領域に記憶する。

[0182] 一致しないと判断する場合には、素数候補生成部142Aは、乱数生成部141Aより受け取った乱数「R1」に2を掛けて、その結果を「R1」として、再度、上記の動作を行い、数「N＝2×R1×q＋1」を生成する。

制御情報が「情報C」でないと判断する場合には、素数候補生成部142Aは、情報

制御部140Aの情報記憶領域より素数「q」及び発行識別子情報「IDI」を読み出す。

素数候補生成部142Aは、制御情報が「情報B」であるか否かを判断する。

[0183] 「情報B」であると判断する場合には、素数候補生成部142Aは、受け取った乱数「R1」と読み出した発行識別子情報「IDI」と関数記憶領域にて記憶している関数「f」とを用いて、数「R＝f(IDI｜｜R1)」を生成する。素数候補生成部142Aは、生成した数「R」と読み出した素数「q」とを用いて、数「N＝2×R×q＋1」を生成する。

[0184] 素数候補生成部142Aは、生成した数「N」のビットサイズ「lenN」が「2×lenq」であるか否かを判断する。

「2×lenq」であると判断する場合には、素数候補生成部142Aは、生成した数「N」を第1素数判定部143Aへ出力し、生成した数「R」を生成情報記憶領域に記憶する。

[0185] 「2×lenq」でないと判断する場合には、素数候補生成部142Aは、乱数生成部141Aより受け取った乱数「R1」に2を掛けて、その結果を「R1」として、再度、数「R」及び「N」を生成する。

「情報B」でないと判断する場合には、素数候補生成部142Aは、受け取った乱数「R1」と読み出した発行識別子情報「IDI」とを用いて、数「R＝IDI×R1」を生成する。

[0186] 素数候補生成部142Aは、情報制御部140Aの検証値記憶領域より検証値「c1」を読み出す。

素数候補生成部142Aは、読み出した素数「q」、発行識別子情報「IDI」、検証値「c1」及び生成した数「R」とを用いて、数「N＝2×(R＋w)×q＋1」を生成する。

[0187] ここで、「w」は「2×w×q＋1＝c1 mod IDI、0≦w＜IDI」を満たす数である。「w」は、「w＝(c1−1)×m mod IDI」を計算することにより求める。「m」は「(2×q)×m＝1 mod IDI」を満たす数である。

素数候補生成部142Aは、素数「q」のビットサイズ「lenq」を、情報制御部140Aの情報記憶領域より読み出し、生成した数「N」のビットサイズが「2×lenq」であるか否かを判断する。

[0188] 「2×lenq」であると判断する場合には、素数候補生成部142Aは、生成した数「N」を第1素数判定部143Aへ出力し、生成した数「R」を生成情報記憶領域に記憶する

。

「2×lenq」でないと判断する場合には、素数候補生成部142Aは、乱数生成部141Aより受け取った乱数「R1」に2を掛けて、その結果を「R1」として、再度、数「R」及び「N」を生成する。

[0189] ＜第1素数判定部143A＞

第1素数判定部143Aは、第1の実施の形態にて示す第1素数判定部143と同様であるため、説明は省略する。

＜第2素数判定部144A＞

第2素数判定部144Aは、第1の実施の形態にて示す第2素数判定部144と同様であるため、説明は省略する。

[0190] (2)発行公開鍵確認部214A

発行公開鍵確認部214Aは、図示していないが、サーバ情報記憶領域220A及び確認情報記憶領域221Aを有している。

サーバ情報記憶領域220Aは、公開鍵証明書の発行依頼のあった鍵発行サーバを識別するサーバ識別子を記憶する領域を有している。

[0191] 確認情報記憶領域221Aは、図20に示すように、検証値テーブルT250を有している。検証値テーブルT250は、サーバ識別子と、検証値とからなる組を1以上記憶する領域を有している。サーバ識別子は、鍵発行サーバを識別する識別子であり、「SIDA」は、鍵発行サーバ100を示し、「SIDB」は、鍵発行サーバ101を示し、「SIDB」は、鍵発行サーバ102を示す。検証値は、対応付けられたサーバ識別子にて示される鍵発行サーバに割り当てた検証値である。なお、以降では、鍵発行サーバ100のサーバ識別子を「SID」として説明する。

[0192] 発行公開鍵確認部214Aは、鍵発行サーバ100から受信部217を介して、発行識別子情報「IDI」と、公開鍵「PK」と、サーバ識別子と、証明書発行依頼情報とを受け取る。

発行公開鍵確認部214Aは、受け取ったサーバ識別子を、サーバ情報記憶領域220Aに書き込む。

[0193] 発行公開鍵確認部214Aは、受け取ったサーバ識別子を用いて、対応する検証値

「c1」を読み出す。

発行公開鍵確認部214Aは、受け取った公開鍵「PK」と発行識別子情報「IDI」とを用いて、公開鍵「PK」が、発行識別子情報「IDI」を用いて生成されたか否かを確認する。

[0194] ここで、確認方法は、「n−(c1)^2」が、「IDI」で割り切れるか否かを検証する。これにより、公開鍵「PK」が、発行識別子情報「IDI」を用いて生成されたか否かを確認することができる。

発行公開鍵確認部214Aは、「n−(c1)^2」が、「IDI」で割り切れると判断する場合には、公開鍵「PK」が、発行識別子情報「IDI」を用いて生成されたと判断し、「n−(c1)^2」が、「IDI」で割り切れないと判断する場合には、公開鍵「PK」が、発行識別子情報「IDI」を用いて生成されていないと判断する。

[0195] 発行公開鍵確認部214Aは、公開鍵「PK」が、発行識別子情報「IDI」を用いて生成されたと判断する場合には、受け取った公開鍵「PK」を発行公開鍵格納部211へ、発行識別子情報を発行識別子情報格納部212へ、それぞれ書き込む。発行公開鍵確認部214Aは、公開鍵証明書の生成開始命令を公開鍵証明書生成部215へ出力する。

発行公開鍵確認部214Aは、公開鍵「PK」が、発行識別子情報「IDI」を用いて生成されていないと判断する場合には、処理を終了する。

[0196] (3)素数候補生成処理

本変形例に係る素数候補生成処理について、第1実施の形態にて示した素数候補生成処理と異なる点のみ説明する。なお、鍵発行処理、及び素数生成処理の動作の流れは、第1の実施の形態と同様であるため、説明は省略する。

素数候補生成部142Aは、図16及び図17に示すステップS500からステップS560までを実行後、ステップS565を省略して、ステップS570にて、検証値「c1」を読み出す。素数候補生成部142Aは、ステップS575にて、数「N＝2×(R＋w)×q＋1」を生成する。つまり、ステップS565、ステップS580及びステップS585を省略し、ステップS570及びステップS575を上記のように変更する。

[0197] 以降は、第1の実施の形態と同様であるため、説明は省略する。

つまり、本変形例に係る素数候補生成処理は、出力カウンタの値に関わらず、検証値「c1」と素数「q」と数「R」とを用いて、数「N」を生成することになる。

(4)証明書発行処理

本変形例に係る証明書発行処理について、第1実施の形態にて示した証明書発行処理と異なる点のみ説明する。

[0198] 発行公開鍵確認部214Aは、ステップS660にて、受け取ったサーバ識別子に対応する検証値(例えば、「c1」)を読み出し、ステップS670にて、読み出した検証値「c1」と、公開鍵「PK」と発行識別子情報「IDI」とを用いて、「PK」が「IDI」より生成されたか否かを確認する。

1.11 素数生成の変形例2

上記実施の形態では、第1検証値及び第2検証値の2つの検証値を用いたが、ここでは、1個の検証値であり、且つその検証値が固定値「1」である場合の素数の生成について、説明する。

[0199] 上記実施の形態と異なる点は、鍵発行サーバにおける素数情報生成部と、証明書発行サーバにおける発行公開鍵確認部とが異なる。以下に、本変形例における素数情報生成部133B、及び発行公開鍵確認部214Bについて説明する。なお、他の構成要素については、第1の実施の形態にて示した構成要素を用いる。

(1)素数情報生成部133B

素数情報生成部133Bは、図21に示すように、情報制御部140B、乱数生成部141B、素数候補生成部142B、第1素数判定部143B及び第2素数判定部144Bから構成されている。

[0200] 素数情報生成部133Bは、繰返制御部132から受け取った素数のビットサイズが2倍のビットサイズからなる素数を生成する。

なお、以下の説明において、繰返制御部132から受け取る素数を素数「q」、そのビットサイズを「lenq」として、各構成要素について説明する。

＜情報制御部140B＞

情報制御部140Bは、第1情報及び第2情報を記憶するための情報記憶領域を有している。

[0201] 情報制御部140Bは、制御情報「情報A」に基づいて素数を生成する際に用いる検証値「1」を予め記憶している検証値記憶領域を有している。

情報制御部140Bは、繰返制御部132から、素数「q」と、素数のビットサイズ「lenq」と、制御情報とからなる第1情報を受け取ると、受け取った第1情報を情報記憶領域へ書き込む。つまり、素数「q」と、素数のビットサイズ「lenq」と、制御情報(この場合、「情報C」)とを書き込む。

[0202] 情報制御部140Bは、繰返制御部132から、素数「q」と、素数のビットサイズ「lenq」と、制御情報と、発行識別子情報「IDI」と、そのビットサイズ「lenIDI」とからなる第2情報を受け取ると、受け取った第2情報を情報記憶領域へ書き込む。つまり、素数「q」と、素数のビットサイズ「lenq」と、制御情報、発行識別子情報「IDI」と、そのビットサイズ「lenIDI」とを書き込む。

[0203] 情報制御部140Bは、受け取った情報の書き込み後、乱数の生成の指示を示す第1生成指示を、乱数生成部141Bへ出力する。

情報制御部140Bは、第2素数判定部144Bより、素数を受け取ると、受け取った素数を繰返制御部132へ出力する。

＜乱数生成部141B＞

乱数生成部141Bは、第1の実施の形態にて示す乱数生成部141Bと同様であるため、説明は省略する。

[0204] ＜素数候補生成部142B＞

素数候補生成部142Bは、生成された情報を記憶する生成情報記憶領域と、単射である関数「f」を予め記憶している関数記憶領域とを有している。

素数候補生成部142Bは、乱数生成部141Bより、乱数「R1」と制御情報とを受け取ると、受け取った制御情報が「情報C」であるか否かの判断をする。

[0205] 「情報C」であると判断する場合には、素数候補生成部142Bは、情報制御部140Bの情報記憶領域より素数「q」を読み出す。素数候補生成部142Bは、読み出した素数「q」と乱数生成部141Bより受け取った乱数「R1」とを用いて、数「N＝2×R1×q＋1」を生成する。素数候補生成部142Bは、生成した数「N」のビットサイズ「lenN」が「lenq」と一致するか否かを判断し、一致すると判断する場合には、素数候補生成

部142Bは、生成した数「N」を第1素数判定部143Bへ出力し、受け取った乱数「R1」を、「R」として生成情報記憶領域に記憶する。

[0206] 一致しないと判断する場合には、素数候補生成部142Bは、乱数生成部141Bより受け取った乱数「R1」に2を掛けて、その結果を「R1」として、再度、上記の動作を行い、数「N＝2×R1×q＋1」を生成する。

制御情報が「情報C」でないと判断する場合には、素数候補生成部142Bは、情報制御部140Bの情報記憶領域より素数「q」及び発行識別子情報「IDI」を読み出す。素数候補生成部142Bは、制御情報が「情報B」であるか否かを判断する。

[0207] 「情報B」であると判断する場合には、素数候補生成部142Bは、受け取った乱数「R1」と読み出した発行識別子情報「IDI」と関数記憶領域にて記憶している関数「f」とを用いて、数「R＝f(IDI｜｜R1)」を生成する。素数候補生成部142Bは、生成した数「R」と読み出した素数「q」とを用いて、数「N＝2×R×q＋1」を生成する。

[0208] 素数候補生成部142Bは、生成した数「N」のビットサイズ「lenN」が「2×lenq」であるか否かを判断する。

「2×lenq」であると判断する場合には、素数候補生成部142Bは、生成した数「N」を第1素数判定部143Bへ出力し、生成した数「R」を生成情報記憶領域に記憶する。

[0209] 「2×lenq」でないと判断する場合には、素数候補生成部142Bは、乱数生成部141Bより受け取った乱数「R1」に2を掛けて、その結果を「R1」として、再度、数「R」及び「N」を生成する。

「情報B」でないと判断する場合には、素数候補生成部142Bは、受け取った乱数「R1」と読み出した発行識別子情報「IDI」とを用いて、数「R＝IDI×R1」を生成する。

[0210] 素数候補生成部142Bは、情報制御部140Bの検証値記憶領域より検証値「1」を読み出す。

素数候補生成部142Bは、読み出した素数「q」、発行識別子情報「IDI」、検証値「1」及び生成した数「R」とを用いて、数「N＝2×R×q＋1」を生成する。ここで、最後の項の「1」が検証値である。

[0211] 素数候補生成部142Bは、素数「q」のビットサイズ「lenq」を、情報制御部140Bの

情報記憶領域より読み出し、生成した数「N」のビットサイズが「2×lenq」であるか否かを判断する。

「2×lenq」であると判断する場合には、素数候補生成部142Bは、生成した数「N」を第1素数判定部143Bへ出力し、生成した数「R」を生成情報記憶領域に記憶する。

[0212] 「2×lenq」でないと判断する場合には、素数候補生成部142Bは、乱数生成部141Bより受け取った乱数「R1」に2を掛けて、その結果を「R1」として、再度、数「R」及び「N」を生成する。

＜第1素数判定部143B＞

第1素数判定部143Bは、第1の実施の形態にて示す第1素数判定部143と同様であるため、説明は省略する。

[0213] ＜第2素数判定部144B＞

第2素数判定部144Bは、第1の実施の形態にて示す第2素数判定部144と同様であるため、説明は省略する。

(2)発行公開鍵確認部214B

発行公開鍵確認部214Bは、図示していないが、サーバ情報記憶領域220B及び確認情報記憶領域221Bを有している。

[0214] サーバ情報記憶領域220Bは、公開鍵証明書の発行依頼のあった鍵発行サーバを識別するサーバ識別子を記憶する領域を有している。

確認情報記憶領域221Bは、固定値である検証値「1」を記憶している。

発行公開鍵確認部214Bは、鍵発行サーバ100から受信部217を介して、発行識別子情報「IDI」と、公開鍵「PK」と、サーバ識別子と、証明書発行依頼情報とを受け取る。

[0215] 発行公開鍵確認部214Bは、受け取ったサーバ識別子を、サーバ情報記憶領域220Bに書き込む。

発行公開鍵確認部214Bは、検証値「1」を、確認情報記憶領域221Bから読み出す。

発行公開鍵確認部214Bは、受け取った公開鍵「PK」と発行識別子情報「IDI」とを

用いて、公開鍵「PK」が、発行識別子情報「IDI」を用いて生成されたか否かを確認する。

[0216] ここで、確認方法は、「n−検証値」、つまり「n−1」が、「IDI」で割り切れるか否かを検証する。これにより、公開鍵「PK」が、発行識別子情報「IDI」を用いて生成されたか否かを確認することができる。

発行公開鍵確認部214Bは、「n−1」が、「IDI」で割り切れると判断する場合には、公開鍵「PK」が、発行識別子情報「IDI」を用いて生成されたと判断し、「n−1」が、「IDI」で割り切れないと判断する場合には、公開鍵「PK」が、発行識別子情報「IDI」を用いて生成されていないと判断する。

[0217] 発行公開鍵確認部214Bは、公開鍵「PK」が、発行識別子情報「IDI」を用いて生成されたと判断する場合には、受け取った公開鍵「PK」を発行公開鍵格納部211へ、発行識別子情報を発行識別子情報格納部212へ、それぞれ書き込む。発行公開鍵確認部214Bは、公開鍵証明書の生成開始命令を公開鍵証明書生成部215へ出力する。

発行公開鍵確認部214Bは、公開鍵「PK」が、発行識別子情報「IDI」を用いて生成されていないと判断する場合には、処理を終了する。

[0218] (3)素数候補生成処理

本変形例に係る素数候補生成処理について、第1実施の形態にて示した素数候補生成処理と異なる点のみ説明する。なお、鍵発行処理、及び素数生成処理の動作の流れは、第1の実施の形態と同様であるため、説明は省略する。

素数候補生成部142Bは、図16及び図17に示すステップS500からステップS560までを実行後、ステップS565を省略して、ステップS570にて、検証値「1」を読み出す。素数候補生成部142Bは、ステップS575にて、数「N＝2×(R＋w)×q＋1」を生成する。つまり、ステップS565、ステップS580及びステップS585を省略し、ステップS570及びステップS575を上記のように変更する。なお、数「N」を算出する際の最後の項が検証値である。

[0219] 以降は、第1の実施の形態と同様であるため、説明は省略する。

つまり、本変形例に係る素数候補生成処理は、出力カウンタの値に関わらず、素数

「q」と数「R」とを用いて、数「N」を生成することになる。

(4)証明書発行処理

本変形例に係る証明書発行処理について、第1実施の形態にて示した証明書発行処理と異なる点のみ説明する。

[0220] 発行公開鍵確認部214Bは、ステップS660にて、検証値「1」を読み出し、ステップS670にて、読み出した検証値「1」と、公開鍵「PK」と発行識別子情報「IDI」とを用いて、「PK」が「IDI」より生成されたか否かを確認する。

(5)確認方法の検証

上記に示した方法にて、証明書発行サーバは、鍵発行サーバが正しく発行識別子情報IDIを用いて生成しているかを確認することができる。

[0221] なぜなら、秘密鍵である素数「p1」、「p2」はそれぞれ、素数「q1」、「q2」、乱数「R11」、「R12」、発行識別子情報「IDI」を用いて、「p1＝2×q1×IDI×R11＋1」、「p2＝2×q2×IDI×R12＋1」を満たすため、

$$n=p1\times p2=(2\times q1\times IDI\times R11+1)\times(2\times q2\times IDI\times R12+1)$$
$$=IDI\times(4\times q1\times q2\times R11\times R12\times IDI+2\times q1\times R11+2\times q2\times R12)+1$$

となる。そのため、「n−1」は「IDI」で割り切れるため、「n−1」が「IDI」で割り切れることを確認することで、素数「p1」、「p2」が正しく発行識別子情報「IDI」を用いて生成しているかを確認することができる。

[0222] 1．12 素数生成の変形例3

上記実施の形態では、256ビットの素数を生成する際に、単射関数を施して、生成する素数の一意性を満たし、512ビットの素数を生成する際に、生成する素数の正当性を確認するための要素を付加したが、ここでは、素数の一意性及び正当性を確認するための要素の付加を、1回の動作にて行う場合について、説明する。

[0223] 上記実施の形態と異なる点は、鍵発行サーバにおける素数生成部と、証明書発行サーバにおける発行公開鍵確認部とが異なる。以下に、本変形例における素数生成部116C、及び発行公開鍵確認部214Cについて説明する。なお、他の構成要素については、第1の実施の形態にて示した構成要素を用いる。

また、ここでは、サーバ識別子のビットサイズを15ビット、端末装置の端末識別子のビットサイズを16ビットとし、発行識別子情報のビットサイズを32ビットする。

[0224] (1)素数生成部116C

素数生成部116Cは、図22に示すように、繰返制御部132C及び素数情報生成部133Cとを有している。

素数生成部116Cは、8ビットの素数から512ビットの素数を生成し、生成した512ビットの素数を鍵判定部117へ出力する。

[0225] <繰返制御部132C>

繰返制御部132Cは、8ビットからなる素数とその素数のビットサイズ(つまり「8」)とを予め記憶している初期値記憶領域と、素数情報生成部133Cから、受け取った素数を一時的に記憶する一時記憶領域とを有している。

繰返制御部132Cは、素数情報生成部133Cの動作の繰返回数をカウントする繰返カウンタ135Cと、鍵判定部117へ出力した素数の個数、つまり生成した512ビットの素数の出力回数をカウントする出力カウンタ136Cとを有している。なお、繰返カウンタ135C及び出力カウンタ136Cの初期値は、それぞれ「1」である。

[0226] 繰返制御部132Cは、図23に示す制御情報テーブルT150を有している。制御情報テーブルT150は、回数と制御情報とからなる組を1以上格納している。回数は、繰返カウンタ135Cの値に対応する。制御情報は、素数情報生成部133Cにて生成する素数の生成方法の種別を示す。

繰返制御部132Cは、識別子生成部115から素数の生成開始命令を受け取ると、素数情報生成部133Cが素数を生成するよう制御する。素数情報生成部133Cから素数を受け取ると、繰返カウンタ135C及び出力カウンタ136Cのそれぞれの値に基づいて、再度、素数情報生成部133Cへ素数生成の命令、及び受け取った素数を鍵判定部117へ出力の何れかを行う。

[0227] 以下に、その動作について説明する。

繰返制御部132Cは、識別子生成部115から素数の生成開始命令を受け取ると、繰返カウンタ135C及び出力カウンタ136Cを、それぞれ「1」に設定する。

繰返制御部132Cは、素数情報生成部133Cから、素数を受け取ると、繰返カウン

タ135Cの値に「1」を加算し、加算結果が、7であるか否かを判断する。

[0228] 加算結果が7であると判断する場合には、繰返制御部132Cは、出力カウンタ136Cの値が、1であるか否かを判断する。1であると判断する場合には、繰返制御部132Cは、受け取った素数を素数「p1」として、鍵判定部117へ出力し、出力カウンタ136Cの値に「1」を加算し、繰返カウンタ135Cの値に「1」を設定する。1でない、つまり2以上であると判断する場合には、繰返制御部132Cは、受け取った素数を素数「p2」として、素数「p2」と判定開始命令を鍵判定部117へ出力する。

[0229] 加算結果が7でないと判断する場合には、受け取った素数のビットサイズを算出し、受け取った素数と、算出したビットサイズとを、一時記憶領域に一時的に記憶する。

繰返制御部132Cは、素数の生成開始命令を受け取り、繰返カウンタ135C及び出力カウンタ136Cのそれぞれの値に「1」を加算した後、素数情報生成部133Cから受け取った素数とそのビットサイズとを一時的に記憶した後、及び出力カウンタ136Cに「1」を加算し、且つ繰返カウンタ135Cの値を「1」に設定した後の何れかの場合において、繰返制御部132Cは、以下の動作を行う。

[0230] 繰返制御部132Cは、繰返カウンタ135Cの値が、1であるか否かを判断する。1であると判断する場合には、繰返制御部132Cは、初期値記憶領域より8ビットの素数とそのビットサイズを読み出し、1でないと判断する場合には、一時記憶領域よりビットサイズ「8×(2^(n−1))」と、その素数とを読み出す。つまり、繰返制御部132Cは、繰返カウンタ135Cの値が、1でないと判断する場合には、一時記憶領域より、前回生成した素数とそのビットサイズとを読み出す。ここで、「n」は、繰返カウンタの値である。

[0231] 繰返カウンタ135Cの値に対応する制御情報を制御情報テーブルT150より読み出し、読み出した制御情報が、「情報C」であるか否かを判断する。

「情報C」であると判断する場合には、繰返制御部132Cは、読み出した素数及びそのビットサイズと、制御情報とからなる第1情報を生成し、生成した第1情報を、素数情報生成部133Cへ出力する。

[0232] 「情報C」でないと判断する場合には、繰返制御部132Cは、識別子格納部110より発行識別情報「IDI」を取得し、取得した発行識別子情報「IDI」のビットサイズ「lenID

I」を算出し、読み出した素数及びそのビットサイズと、制御情報と、発行識別子情報「IDI」及びそのビットサイズ「lenIDI」とからなる第2情報を生成し、生成した第2情報を、素数情報生成部133Cへ出力する。

[0233] また、繰返制御部132Cは、鍵判定部117より素数を再度生成する旨の再生成命令を受け取ると、出力カウンタ136Cの値に「1」を加算し、且つ繰返カウンタ135Cの値を「1」に設定し、繰返カウンタ135Cの値が、1であるか否かの判断を行う動作以降を行う。

＜素数情報生成部133C＞

素数情報生成部133Cは、図24に示すように、情報制御部140C、乱数生成部141C、素数候補生成部142C、第1素数判定部143C及び第2素数判定部144Cから構成されている。

[0234] 素数情報生成部133Cは、繰返制御部132Cから受け取った素数のビットサイズが2倍のビットサイズからなる素数を生成する。例えば、8ビットからなる素数を受け取った場合には、16ビットからなる素数を生成し、16ビットからなる素数を受け取った場合には、32ビットからなる素数を生成する。

なお、以下の説明において、繰返制御部132Cから受け取る素数を素数「q」、そのビットサイズを「lenq」として、各構成要素について説明する。

[0235] ＜情報制御部140C＞

情報制御部140Cは、第1情報及び第2情報を記憶するための情報記憶領域を有している。

情報制御部140Cは、証明書発行サーバ200により割り当てられ、且つ制御情報「情報AB」に基づいて素数を生成する際に用いる素数「qg」とそのビットサイズ「lenqg」とを予め記憶している割当素数記憶領域を有している。ここで、素数「qg」のビットサイズは、例えば、「64」ビットである。

[0236] 情報制御部140Cは、繰返制御部132Cから、素数「q」と、素数のビットサイズ「lenq」と、制御情報とからなる第1情報を受け取ると、受け取った第1情報を情報記憶領域へ書き込む。つまり、素数「q」と、素数のビットサイズ「lenq」と、制御情報（この場合、「情報C」）とを書き込む。

情報制御部140Cは、繰返制御部132Cから、素数「q」と、素数のビットサイズ「lenq」と、制御情報と、発行識別子情報「IDI」と、そのビットサイズ「lenIDI」とからなる第2情報を受け取ると、受け取った第2情報を情報記憶領域へ書き込む。つまり、素数「q」と、素数のビットサイズ「lenq」と、制御情報、発行識別子情報「IDI」と、そのビットサイズ「lenIDI」とを書き込む。

[0237] 情報制御部140Cは、受け取った情報の書き込み後、乱数の生成の指示を示す第1生成指示を、乱数生成部141Cへ出力する。

情報制御部140Cは、第2素数判定部144Cより、素数を受け取ると、受け取った素数を繰返制御部132Cへ出力する。

情報制御部140Cは、素数候補生成部142Cから出力カウンタ136Cの値を読み出す旨の回数読出命令を受け取ると、繰返制御部132Cの出力カウンタ136Cの値を読み出す。情報制御部140Cは、読み出した値を、素数候補生成部142Cへ出力する。

[0238] ＜乱数生成部141C＞

乱数生成部141Cは、乱数の生成の指示を示す第1生成指示を、情報制御部140Cから受け取ると、情報制御部140Cの情報記憶領域にて記憶されている制御情報を読み出す。乱数生成部141Cは、読み出した制御情報が「情報C」であるか否かを判断する。

[0239] 「情報C」であると判断する場合には、乱数生成部141Cは、情報制御部140Cの情報記憶領域にて記憶されている「lenq」を読み出し、(lenq−1)ビットからなる乱数「R1」を生成し、生成した乱数「R1」と読み出した制御情報とを素数候補生成部142Cへ出力する。ここで、乱数「R1」の最上位ビットは1とする。乱数生成方法は、非特許文献2が詳しい。

[0240] 「情報C」でないと判断する場合には、乱数生成部141Cは、情報制御部140Cの情報記憶領域にて記憶されている「lenq」を、割当素数記憶領域にて記憶されている「lenqg」を、それぞれ読み出す。乱数生成部141Cは、読み出した「lenq」及び「lenqg」を用いて、(lenq−2×lenqg−1)ビットからなる乱数「R1」を生成し、生成した乱数「R1」と読み出した制御情報とを素数候補生成部142Cへ出力する。ここで、乱数

「R1」の最上位ビットは1とする。

[0241] また、乱数生成部141Cは、第1素数判定部143及び第2素数判定部144の何れかから、再度乱数を生成する旨の第2生成指示を受け付けると、制御情報を情報記憶領域より読み出し、上記の動作を行う。

＜素数候補生成部142C＞

素数候補生成部142Cは、生成された情報を記憶する生成情報記憶領域と、発行識別子情報「IDI」と素数「qg」とから一意的に素数を生成する素数生成関数「gp」、及び単射である関数「f」を予め記憶している関数記憶領域とを有している。

[0242] ここで、素数生成関数「gp」を用いた素数生成の一例を、以下に示す。

先ず、「c＝0」として、「2×qg×f(IDI｜｜c)＋1」が素数であるかを判定する。素数である場合は、「gp(IDI, qg)＝2×qg×f(IDI｜｜c)＋1」とする。素数でなければ、「c」に「1」加算して、「2×qg×f(IDI｜｜c)＋1」が素数であるかを判定する。素数であれば、「gp(IDI, qg)＝2×qg×f(IDI｜｜c)＋1」とする。素数でなければ、「c」に「1」加算して同様の判定を行い素数になるまで繰り返す。このように関数「gp」を定義するとき、関数「qg」と「f」とを保持していれば、発行識別子情報「IDI」に対して、素数候補生成部142Cは、何回素数生成関数により素数を生成しても、同じ素数を生成するができる。このとき、「IDI」のビットサイズ及び「qg」のビットサイズが、それぞれ「32」ビット及び「64」ビットである場合には、「gp(IDI、qg)」のビットサイズは、128ビットとなる。

[0243] 素数候補生成部142Cは、乱数生成部141Cより、乱数「R1」と制御情報とを受け取ると、受け取った制御情報が「情報C」であるか否かの判断をする。

「情報C」であると判断する場合には、素数候補生成部142Cは、情報制御部140Cの情報記憶領域より素数「q」を読み出す。素数候補生成部142Cは、読み出した素数「q」と乱数生成部141Cより受け取った乱数「R1」とを用いて、数「N＝2×R1×q＋1」を生成する。素数候補生成部142Cは、生成した数「N」のビットサイズ「lenN」が「lenq」と一致するか否かを判断し、一致すると判断する場合には、素数候補生成部142Cは、生成した数「N」を第1素数判定部143Cへ出力し、受け取った乱数「R1」を、「R」として生成情報記憶領域に記憶する。

[0244] 一致しないと判断する場合には、素数候補生成部142Cは、乱数生成部141より受け取った乱数「R1」に2を掛けて、その結果を「R1」として、再度、上記の動作を行い、数「N＝2×R1×q＋1」を生成する。

制御情報が「情報C」でないと判断する場合、つまり制御情報が「情報AB」であると判断する場合には、素数候補生成部142Cは、情報制御部140Cの情報記憶領域より素数「q」及び発行識別子情報「IDI」を、割当素数記憶領域より素数「qg」を、それぞれ読み出す。

[0245] 素数候補生成部142Cは、読み出した発行識別子情報「IDI」及び素数「qg」と、関数記憶領域にて記憶している関数「f」及び「gp」とを用いて、上記に示す方法にて、素数「pIDI＝gp(IDI、qg)」を生成し、生成した素数「pIDI」を生成情報記憶領域へ記憶する。

素数候補生成部142Cは、生成情報記憶領域にて記憶している素数「pIDI」を読み出し、読み出した素数「pIDI」と、受け取った乱数「R1」と、読み出した素数「q」とを用いて、数「N＝2×R1×q×pIDI＋1」を生成する。

[0246] 素数候補生成部142Cは、生成した数「N」のビットサイズ「lenN」が「2×lenq」であるか否かを判断する。

「2×lenq」であると判断する場合には、素数候補生成部142Cは、生成した数「N」を第1素数判定部143Cへ出力し、受け取った乱数「R1」を「R」として生成情報記憶領域に記憶する。

[0247] 「2×lenq」でないと判断する場合には、素数候補生成部142Cは、乱数生成部141Cより受け取った乱数「R1」に2を掛けて、その結果を「R1」として、再度、数「N」を生成する。

＜第1素数判定部143C＞

第1素数判定部143Cは、第1の実施の形態にて示す第1素数判定部143と同様であるため、説明は省略する。

[0248] ＜第2素数判定部144C＞

第2素数判定部144Cは、第1の実施の形態にて示す第1素数判定部144と同様であるため、説明は省略する。

(2)発行公開鍵確認部214C

発行公開鍵確認部214Cは、図示していないが、サーバ情報記憶領域220C及び確認情報記憶領域221Cを有している。

[0249] サーバ情報記憶領域220Cは、公開鍵証明書の発行依頼のあった鍵発行サーバを識別するサーバ識別子を記憶する領域を有している。

確認情報記憶領域221Cは、鍵発行サーバ100に割り当てた素数「qg」とそのビットサイズ「lenqg」と、鍵発行サーバ100にて記憶している素数生成関数及び単射関数のそれぞれと同様の関数「gp」及び「f」を予め記憶している。

[0250] 発行公開鍵確認部214Cは、鍵発行サーバ100から受信部217を介して、発行識別子情報「IDI」と、公開鍵「PK＝(n、e)」と、サーバ識別子と、証明書発行依頼情報とを受け取る。

発行公開鍵確認部214Cは、受け取ったサーバ識別子を、サーバ情報記憶領域220Cに書き込む。

[0251] 発行公開鍵確認部214Cは、受け取った公開鍵「PK」と発行識別子情報「IDI」とを用いて、公開鍵「PK」が、発行識別子情報「IDI」を用いて生成されたか否かを確認する。

以下に、確認方法を示す。先ず、発行公開鍵確認部214Cは、受け取った発行識別子情報「IDI」と、記憶している素数「qg」、関数「gp」及び「f」とを用いて、素数「gp(IDI、qg)」を生成し、生成した素数素数「gp(IDI、qg)」を確認情報記憶領域221Cへ書き込む。素数「gp(IDI、qg)」の生成方法は、上記に示す方法と同様であるため、説明は省略する。このとき、発行公開鍵確認部214Cにて生成される素数「gp(IDI、qg)」は、鍵発行サーバの素数候補生成部142Cにて生成される素数「pIDI」と同じであることが分かる。

[0252] 次に、発行公開鍵確認部214Cは、確認情報記憶領域221Cにて記憶している素数「gp(IDI、qg)」を読み出し、「n−1」が、読み出した素数「gp(IDI、qg)」で割り切れるか否かを検証する。これにより、公開鍵「PK」が、発行識別子情報「IDI」を用いて生成されたか否かを確認することができる。

発行公開鍵確認部214Cは、「n−1」が、素数「gp(IDI、qg)」で割り切れると判断す

る場合には、公開鍵「PK」が、発行識別子情報「IDI」を用いて生成されたと判断し、「n−1」が、素数「gp(IDI、qg)」で割り切れないと判断する場合には、公開鍵「PK」が、発行識別子情報「IDI」を用いて生成されていないと判断する。

[0253] 発行公開鍵確認部214Cは、公開鍵「PK」が、発行識別子情報「IDI」を用いて生成されたと判断する場合には、受け取った公開鍵「PK」を発行公開鍵格納部211へ、発行識別子情報を発行識別子情報格納部212へ、それぞれ書き込む。発行公開鍵確認部214Cは、公開鍵証明書の生成開始命令を公開鍵証明書生成部215へ出力する。

発行公開鍵確認部214Cは、公開鍵「PK」が、発行識別子情報「IDI」を用いて生成されていないと判断する場合には、処理を終了する。

[0254] (3)素数生成処理

本変形例に係る素数生成処理について、第1実施の形態にて示した素数生成処理と異なる点のみ説明する。なお、鍵発行処理の動作の流れは、第1の実施の形態と同様であるため、説明は省略する。

図15に示す素数生成処理のステップS425において、乱数生成部141Cは、乱数生成部141Cは、情報制御部140Cの情報記憶領域にて記憶されている「lenq」を、割当素数記憶領域にて記憶されている「lenqg」を、それぞれ読み出すように変更する。次に、ステップS430において、乱数生成部141Cは、読み出した「lenq」及び「lenqg」を用いて、(lenq−2×lenqg−1)ビットからなる乱数「R1」を生成し、生成した乱数「R1」と読み出した制御情報とを素数候補生成部142Cへ出力するように変更する。ここで、乱数「R1」の最上位ビットは1とする。

[0255] (4)素数候補生成処理

本変形例に係る素数候補生成処理について、図25に示す流れ図を用いて説明する。

素数候補生成部142Cは、乱数生成部141Cより、乱数「R1」と制御情報とを受け取ると(ステップS700)、受け取った制御情報が「情報C」であるか否かの判断をする(ステップS705)。

[0256] 「情報C」であると判断する場合には(ステップS705における「YES」)、素数候補生

成部142Cは、情報制御部140Cの情報記憶領域より素数「q」を読み出す(ステップS710)。素数候補生成部142Cは、読み出した素数「q」と乱数生成部141Cより受け取った乱数「R1」とを用いて、数「N＝2×R1×q＋1」を生成する(ステップS715)。素数候補生成部142Cは、生成した数「N」のビットサイズ「lenN」が「lenq」と一致するか否かを判断し(ステップS720)、一致すると判断する場合には(ステップS720における「YES」)、素数候補生成部142Cは、生成した数「N」を第1素数判定部143Cへ出力し、受け取った乱数「R1」を、「R」として生成情報記憶領域に記憶する(ステップS755)。

[0257] 一致しないと判断する場合には(ステップS720における「NO」)、素数候補生成部142Cは、乱数生成部141より受け取った乱数「R1」に2を掛けて、その結果を「R1」とし(ステップS725)、ステップS715へ戻る。

制御情報が「情報C」でないと判断する場合(ステップS705における「NO」)、つまり制御情報が「情報AB」であると判断する場合には、素数候補生成部142Cは、情報制御部140Cの情報記憶領域より素数「q」及び発行識別子情報「IDI」を、割当素数記憶領域より素数「qg」を、それぞれ読み出す(ステップS730)。

[0258] 素数候補生成部142Cは、読み出した発行識別子情報「IDI」及び素数「qg」と、関数記憶領域にて記憶している関数「f」及び「gp」とを用いて、上記に示す方法にて、素数「pIDI＝gp(IDI、qg)」を生成し、生成した素数「pIDI」を生成情報記憶領域へ記憶する(ステップS735)。

素数候補生成部142Cは、生成情報記憶領域にて記憶している素数「pIDI」を読み出し、読み出した素数「pIDI」と、読み出した素数「q」と、生成した素数「pIDI」とを用いて、数「N＝2×R1×q×pIDI＋1」を生成する(ステップS740)。

[0259] 素数候補生成部142Cは、生成した数「N」のビットサイズ「lenN」が「2×lenq」であるか否かを判断する(ステップS745)。

「2×lenq」であると判断する場合には(ステップS745における「YES」)、素数候補生成部142Cは、生成した数「N」を第1素数判定部143Cへ出力し、乱数「R1」を「R」として生成情報記憶領域に記憶する(ステップS755)。

[0260] 「2×lenq」でないと判断する場合には(ステップS745における「NO」)、素数候補

生成部142Cは、乱数生成部141Cより受け取った乱数「R1」に2を掛けて、その結果を「R1」とし(ステップS750)、ステップS740へ戻る。

(5)証明書発行処理

本変形例に係る証明書発行処理について、第1実施の形態にて示した証明書発行処理と異なる点のみ説明する。

[0261] 発行公開鍵確認部214Cは、ステップS660にて、受け取った発行識別子情報「IDI」と、記憶している素数「qg」、関数「gp」及び「f」とを用いて、素数「gp(IDI、qg)」を生成し、確認情報記憶領域221Cへ書き込むように変更する。ステップS665においては、発行公開鍵確認部214Cは、素数「gp(IDI、qg)」を読み出し、受け取った公開鍵「PK」及び発行識別子情報「IDI」と、読み出した素数「gp(IDI、qg)」とを用いて、公開鍵「PK」が、発行識別子情報「IDI」を用いて生成されたか否かを確認する。

[0262] (6)素数の一意性及び確認方法の検証

上記と同様の証明により、素数生成部116Cにて生成される素数の一意性は満たされる。つまり、端末装置ごとに、異なる発行識別子情報が生成されるため、素数生成に用いる関数「f」の単射の性質により、生成される素数も異なる。これにより、端末装置毎に、異なる秘密鍵及びそれに対応する公開鍵を割り当てることができる。

[0263] 上記に示した方法にて、証明書発行サーバは、鍵発行サーバが正しく発行識別子情報IDIを用いて生成しているかを確認することができる。

なぜなら、秘密鍵である素数「p1」、「p2」はそれぞれ、素数「q1」、「q2」、乱数「R11」、「R12」、及び素数「pIDI=gp(IDI、qg)」を用いて、「p1=2×q1×pIDI×R11+1」、「p2=2×q2×pIDI×R12+1」を満たすため、

$$n=p1\times p2=(2\times q1\times pIDI\times R11+1)\times(2\times q2\times pIDI\times R12+1)$$
$$=pIDI\times(4\times q1\times q2\times R11\times R12\times pIDI+2\times q1\times R11+2\times q2\times R12)+1$$

となる。そのため、「n−1」は「pIDI」で割り切れるため、「n−1」が「pIDI」で割り切れることを確認することで、素数「p1」、「p2」が正しく発行識別子情報「IDI」を用いて生成しているかを確認することができる。

[0264] (7)変形例

本発明は、上記の実施の形態に限定されないのはもちろんである。以下のような場合も本発明に含まれる。

上記の変形例では、予め1個の素数「qg」を記憶しているとしたが、これに限定されない。鍵発行サーバは、予め2つの素数「qg1」、「qg2」を記憶しておき、素数「p1」を生成する場合に、素数「qg1」を用い、素数「p2」を生成する場合に、素数「qg2」を用いてもよい。

[0265] また、上記の変形例では、素数「p1」及び「p2」を生成する場合に用いる「pIDI」を同一のものととしたが、これに限定されない。例えば、素数「p1」の生成に用いる「c」の値と、例えば、素数「p2」の生成に用いる「c」の値とを異なるように設定し、素数「p1」及び「p2」を生成する場合に用いる、それぞれの「pIDI」の値を異なるようにしてもよい。

[0266] 2. 第2の実施の形態

本発明に係る第2の実施の形態としての鍵発行システム2について、第1の実施の形態における鍵発行システム1と異なる点を中心に説明する。

2. 1 鍵発行システム2の概要

鍵発行システム2は、図26に示すように、鍵発行サーバ1100、1101、1102と、鍵発行監査サーバ1200と、端末装置1300、1301、・・・、1302、1303、・・・、1304、1305、・・・、1306から構成されている。端末装置の台数は、例えば1000台である。

[0267] 鍵発行サーバ1100、1101及び1102は、それぞれ異なる会社にて管理されている。端末装置1300、1301、・・・、1302は、鍵発行サーバ1100に対して、鍵の発行要求し、端末装置1303、・・・、1304は、鍵発行サーバ1101に対して、鍵の発行要求し、端末装置1305、・・・、1306は、鍵発行サーバ1102に対して、鍵の発行要求をする。なお、端末装置1300、1301、・・・、1302は、鍵発行サーバ1100との間には、安全な通信経路が確立されているものとする。また、端末装置1303、・・・、1304と、鍵発行サーバ1101との間、及び端末装置1305、・・・、1306は、鍵発行サーバ1102との間においても、同様に、安全な通信経路が確立されているものとする。

[0268] また、鍵発行サーバ1100、1101、1102と、鍵発行監査サーバ1200との間においても、同様に、安全な通信経路が確立されているものとする。

なお、以下においては、鍵発行サーバ1100、鍵発行監査サーバ1200、及び端末装置1300を用いて、鍵発行システム2の概要を説明する。

鍵発行サーバ1100は、端末装置1300より鍵の発行要求を受け取ると、RSA暗号における秘密鍵及び公開鍵を生成する。さらに、鍵発行サーバ1100は、生成した公開鍵に対する公開鍵証明書を生成し、生成した公開鍵証明書及び秘密鍵を、端末装置1300へ送信する。なお、ここで、生成する各鍵の鍵長は、1024ビットとする。

[0269] 鍵発行サーバ1100は、鍵発行監査サーバ1200より、発行済みの公開鍵及び発行識別子情報を要求する旨の発行済鍵依頼情報を受信すると、発行した公開鍵と、公開鍵の生成に用いた発行識別子情報とからなる発行済鍵情報を鍵発行監査サーバ1200へ送信する。

鍵発行監査サーバ1200は、鍵発行サーバ1100より発行済公開鍵情報を受け取ると、発行された公開鍵の正当性を監査し、監査結果を表示する。

[0270] 端末装置1300は、公開鍵証明書と、秘密鍵とを、鍵発行サーバ1100より受け取ると、受け取った公開鍵証明書と、秘密鍵とを記憶する。

以降、例えば、端末装置1400のユーザは、先ず、鍵発行サーバ1100より、端末装置1300の公開鍵証明書を入手、又は端末装置1300より公開鍵証明書を入手し、鍵発行サーバ1100が有し、公開鍵証明書の正当性を確認する際に用いる証明書用公開鍵「C_PK」を用いて、公開鍵証明書の正当性を確認し、正当な公開鍵証明書であると判断する場合に、入手した公開鍵証明書を、端末装置1400にて記憶する。端末装置1400は、記憶している公開鍵証明書に含まれる公開鍵を用いて、端末装置1300へ送信する電子メールを暗号化して、暗号化された電子メールを端末装置1300へ送信する。

[0271] 端末装置1300は、端末装置1400より暗号化された電子メールを受信すると、記憶している秘密鍵を用いて、暗号化された電子メールを復号して、復号された電子メールを表示する。

これにより、端末装置1300と端末装置1400との間では、安全にデータのやりとりができるようになる。

[0272] なお、端末装置1301、・・・、1302は、端末装置1300と同様であるため、説明は省

略する。また、鍵発行サーバ1101、及び1102は、鍵発行サーバ1100と同様であるため、説明は省略する。

以降の説明において、各端末装置の代表として端末装置1300を、各鍵発行サーバの代表として鍵発行サーバ1100を用いる。

[0273] 2.2 鍵発行サーバ1100の構成

鍵発行サーバ1100は、図27にて示すように、識別子格納部1110、秘密鍵格納部1111、公開鍵格納部1112、証明書格納部1113、制御部1114、識別子生成部1115、素数生成部1116、鍵判定部1117、鍵生成部1118、情報取得部1119、受信部1120、送信部1121、証明書生成部1122、証明書用秘密鍵格納部1123及び発行済鍵情報格納部1124から構成されている。

[0274] 鍵発行サーバ1100は、具体的には、マイクロプロセッサ、ROM、RAM、ハードディスクユニット、ディスプレイユニット、キーボード、マウスなどから構成されるコンピュータシステムである。前記RAM又は前記ハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することにより、鍵発行サーバ1100は、その機能を達成する。

[0275] なお、鍵発行サーバ1101、及び1102は、鍵発行サーバ1100と同様の構成であるため、説明は省略する。

(1)識別子格納部1110

識別子格納部1110は、第1の実施の形態における識別子格納部1110と同様に、ビットサイズが126ビット以下である発行識別子情報を記憶するための領域を有している。発行識別子情報のビットサイズは、例えば、64ビットである。

[0276] (2)秘密鍵格納部1111

秘密鍵格納部1111は、第1の実施の形態における秘密鍵格納部1111と同様に、素数格納領域と秘密鍵格納領域とを有している。

(3)公開鍵格納部1112

公開鍵格納部1112は、第1の実施の形態における公開鍵格納部112と同様に、公開鍵を記憶するための領域を有している。

[0277] (4)証明書格納部1113

証明書格納部1113は、当該サーバにて生成した証明書発行サーバにて発行された公開鍵証明書を記憶する領域を有している。

(5)証明書用秘密鍵格納部1123

証明書用秘密鍵格納部1123は、公開鍵証明書を生成する際に用いられる証明書用秘密鍵「C__SK」を、予め記憶している。

[0278] (6)制御部1114

制御部1114は、図27に示すように、サーバ識別子記憶領域1130と、端末情報記憶領域1131とを有している。

サーバ識別子記憶領域1130は、当該サーバを識別するサーバ識別子を予め記憶している。例えば、鍵発行サーバ1100は、SIDAを、鍵発行サーバ1101は、SIDBを、鍵発行サーバ1102は、SIDCを記憶している。なお、以降では、鍵発行サーバ1100のサーバサーバ識別子を「SID」として説明する。ここでは、サーバ識別子のビットサイズを31ビットとする。

[0279] 端末情報記憶領域1131は、鍵発行の要求のあった端末装置を識別する端末識別子を記憶する領域を有している。ここで、端末識別子は、例えば、端末装置のシリアル番号である。ここでは、シリアル番号のビットサイズを32ビットする。

制御部1114は、端末装置1300から受信部1120を介して、鍵発行依頼情報と、端末装置1300の端末識別子「TID」とを受け取ると、受け取った端末識別子「TID」を端末情報記憶領域1131へ書き込む。制御部1114は、発行識別子情報の生成命令と、受け取った端末識別子「TID」とを識別子生成部1115へ出力する。

[0280] 制御部1114は、鍵発行監査サーバ1200から受信部1120を介して、発行済鍵依頼情報を受け取ると、鍵情報取得命令を情報取得部1119へ出力する。

(7)識別子生成部1115

識別子生成部1115は、第1の実施の形態における識別子生成部115と同様であるため、説明は省略する。

[0281] (8)素数生成部1116

素数生成部1116は、第1の実施の形態における素数生成部116の素数の生成方法と同様の方法にて、512ビットの素数を生成する。

(9)鍵判定部1117

鍵判定部1117は、第1の実施の形態における鍵判定部117と同様であるため、説明は省略する。

[0282] (10)鍵生成部1118

鍵生成部1118は、鍵判定部1117より鍵生成命令を受け取ると、秘密鍵格納部111の素数記憶領域にて記憶されている2つの素数「p1」及び「p2」を読み出し、読み出した素数「p1」と「p2」との積「n＝p1×p2」を計算する。

鍵生成部118は、乱数「e」を生成し、算出した「n」と、生成した乱数「e」とからなる組「PK＝(n、e)」を公開鍵として生成し、生成した公開鍵「PK」を公開鍵格納部112へ書き込む。ここで、乱数「e」は、従来と同様に、乱数「e」は、数「L」と互いに素であり、「1≦e≦L−1、GCD(e、L)＝1」を満たす。ここで、GCD(e、L)は、eとLの最大公約数を示し、数「L」は、「L＝LCM(p1−1、p2−1)」であり、LCM(p1−1、p2−1)は、「p1−1」と「p2−1」との最小公倍数を示す。

[0283] 鍵生成部1118は、「e×d＝1 mod L」を満たす「d」を算出し、算出した「d」と、素数「p1」及び「p2」とからなる組「SK＝(p1、p2、d)」を秘密鍵として、秘密鍵格納部111の秘密鍵格納領域へ書き込む。鍵生成部118は、公開鍵証明書の生成命令を、証明書生成部1122へ出力する。

(11)証明書生成部1122

証明書生成部1122は、鍵生成部1118より公開鍵証明書の生成命令を受け取ると、証明書用秘密鍵格納部より証明書用秘密鍵「C__SK」を、公開鍵格納部1112より公開鍵「PK」を、識別子格納部1110より発行識別子情報「IDI」を、それぞれ読み出す。

[0284] 証明書生成部1122は、読み出した秘密鍵「C__SK」、公開鍵「PK」及び発行識別子情報「IDI」を用いて、公開鍵証明書「Cert」を生成する。生成する公開鍵証明書「Cert」は、具体的には、「Cert＝n||e||IDI||Sig(C__SK、n||e||IDI)」である。ここで、Sig(K、D)は、データ「D」に対して、秘密鍵「K」を用いたときの署名データである。記号「||」は、ビットまたはバイトの連結である。

[0285] 証明書生成部1122は、生成した公開鍵証明書「Cert」を証明書格納部1113へ書

き込み、公開鍵証明書「Cert」の配布開始命令を情報取得部1119へ出力する。

(12)情報取得部1119

情報取得部1119は、証明書生成部1122から配布開始命令を受け取ると、秘密鍵格納部1111にて記憶している秘密鍵「SK」と、証明書格納部1113にて記憶している公開鍵証明書「Cert」と、制御部1114の端末情報記憶領域1131にて記憶している端末識別子とを、それぞれ読み出し、読み出した秘密鍵「SK」及び公開鍵証明書「Cert」を、読み出した端末識別子に対応する端末装置1300へ送信部1121を介して送信する。

[0286] 情報取得部1119は、秘密鍵「SK」及び公開鍵証明書「Cert」を、端末装置1300へ送信部1121を介して送信した後、公開鍵格納部1112より発行した公開鍵「PK＝(n、e)」を、識別子格納部1110より発行した発行識別子情報「IDI」を、それぞれ読み出し、読み出した公開鍵「PK」及び発行識別子情報「IDI」を1つの組として、発行済鍵情報格納部1124へ書き込む。

[0287] 情報取得部1119は、制御部1114から鍵情報取得命令を受け取ると、発行済鍵情報格納部1124より、全ての発行済鍵情報を読み出す。情報取得部1119は、制御部1114のサーバ識別子記憶領域1130よりサーバ識別子を読み出し、読み出した全ての発行済鍵情報とサーバ識別子とを、送信部1121を介して鍵発行監査サーバ1200へ送信する。

[0288] (13)発行済鍵情報格納部1124

発行済鍵情報格納部1124は、図28に示すように、発行済鍵情報テーブルT1100を有している。

発行済鍵情報テーブルT1100は、発行済公開鍵と、発行済識別子情報とからなる組を1以上記憶するための領域を有している。

[0289] 発行済公開鍵は、当該鍵発行サーバにて発行した公開鍵であり、発行済識別子情報は、公開鍵及びその公開鍵に対応する秘密鍵を生成する際に用いられた発行識別子情報である。

上記により、鍵発行サーバ1100は、発行した公開鍵と、発行した発行識別子情報とを蓄積していくことができる。

[0290] なお、発行済鍵情報格納部1124は、発行済公開鍵情報である発行履歴を格納するために使用するため、電源が切れてもデータが消えない不揮発性メモリ(例えば、ハードディスクなど)でなければならない。

(14)受信部1120

受信部1120は、鍵発行監査サーバ1200及び端末装置1300より情報を受信し、受信した情報を、制御部1114へ出力する。

[0291] (15)送信部1121

送信部1121は、情報取得部1119より、秘密鍵「SK」及び公開鍵証明書「Cert」を受け取り、受け取った各情報を、端末装置1300に送信する。

送信部1121は、情報取得部1119より、1以上の発行済鍵情報とサーバ識別子とを受け取ると、受け取った1以上の発行済鍵情報とサーバ識別子とを鍵発行監査サーバ1200へ送信する。

[0292] 2.3 鍵発行監査サーバ1200

鍵発行監査サーバ1200は、図29に示すように、確認情報格納部1210、発行済鍵情報格納部1211、制御部1212、発行公開鍵確認部1213、受付部1214、監査結果出力部1215、受信部1216及び送信部1217から構成されている。

鍵発行監査サーバ1200は、具体的には、マイクロプロセッサ、ROM、RAM、ハードディスクユニット、ディスプレイユニット、キーボード、マウスなどから構成されるコンピュータシステムである。前記RAM又は前記ハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することにより、鍵発行監査サーバ1200は、その機能を達成する。

[0293] なお、鍵発行サーバ1100から発行済鍵情報を受け取った場合の動作と、他の鍵発行サーバから発行済鍵情報を受け取った場合の動作とは、同じであるため、以降の説明では、鍵発行サーバ100から送信された発行済鍵情報を用いて説明する。

(1)確認情報格納部1210

確認情報格納部1210は、図30に示すように、検証値テーブルT1200を有している。検証値テーブルT1200は、サーバ識別子と、第1検証値と、第2検証値とからなる組を1以上記憶する領域を有している。サーバ識別子は、鍵発行サーバを識別す

る識別子であり、「SIDA」は、鍵発行サーバ1100を示し、「SIDB」は、鍵発行サーバ1101を示し、「SIDB」は、鍵発行サーバ1102を示す。第1検証値及び第2検証値は、対応付けられたサーバ識別子にて示される鍵発行サーバに割り当てた検証値である。なお、以降では、鍵発行サーバ1100のサーバ識別子を「SID」として説明する。

[0294] (2)発行済鍵情報格納部1211

発行済鍵情報格納部1211は、鍵発行サーバ1100より送信された1以上の発行済鍵情報を記憶するための領域を有している。

(3)制御部1212

制御部1212は、図29に示すように、サーバ情報記憶領域1220を有している。

[0295] サーバ情報記憶領域220は、公開鍵証明書の発行依頼のあった鍵発行サーバを識別するサーバ識別子を記憶する領域を有している。

制御部1212は、受付部1214より、公開鍵の監査を開始する監査開始命令と、監査対象のサーバ識別子(ここでは、「SID」とする。)を受け付けると、発行済鍵依頼情報を、送信部1217を介してサーバ識別子に対応する鍵発行サーバ1100へ送信する。

[0296] 制御部1212は、受付部1214より受け取ったサーバ識別子をサーバ情報記憶領域1220へ書き込む。

制御部1212は、鍵発行サーバ1100から受信部217を介して、1以上の発行済鍵情報とサーバ識別子とを受け取る。

制御部1212は、受け取ったサーバ識別子と、サーバ情報記憶領域にて記憶しているサーバ識別子とが一致するか否かを判断する。

[0297] 一致すると判断する場合には、制御部1212は、受け取った1以上の発行済鍵情報を発行済鍵情報格納部1211へ書き込み、監査開始命令と受け取ったサーバ識別子とを発行公開鍵確認部1213へ出力する。

一致しないと判断する場合には、制御部1212は、処理を終了する。

(4)発行公開鍵確認部1213

発行公開鍵確認部1213は、制御部1212より監査開始命令とサーバ識別子とを受

け取ると、受け取ったサーバ識別子を用いて、対応する第1検証値「c11」及び第2検証値「c12」を、確認情報格納部1210から読み出す。

[0298] 発行公開鍵確認部1213は、未読の発行済鍵情報のうち1つの発行済鍵情報を、発行済鍵情報格納部1211から読み出す。

発行公開鍵確認部1213は、読み出した発行済鍵情報に含まれる公開鍵「PK」と発行識別子情報「IDI」と、第1検証値「c11」及び第2検証値「c12」とを用いて、公開鍵「PK」が、発行識別子情報「IDI」を用いて生成されたか否かを確認する。

[0299] ここで、確認方法は、第1の実施の形態と同様であるため、説明は省略する。

発行公開鍵確認部1213は、「n−(c11×c12)」が、「IDI」で割り切れると判断する場合には、公開鍵「PK」が、発行識別子情報「IDI」を用いて生成されたと判断し、「n−(c11×c12)」が、「IDI」で割り切れないと判断する場合には、公開鍵「PK」が、発行識別子情報「IDI」を用いて生成されていないと判断し、読み出した発行識別子情報「IDI」を一時的に記憶する。

[0300] 発行公開鍵確認部1213は、未読の発行済鍵情報が存在するか否かを判断し、未読の発行済鍵情報が存在すると判断する場合には、上記の動作を繰り返す。未読の発行済鍵情報が存在しないと判断する場合には、一時的に記憶している発行識別子情報が存在するか否かを判断する。

一時的に記憶している発行識別子情報が存在すると判断する場合には、発行公開鍵確認部1213は、記憶されている全ての発行識別子を連結し、不正発行識別子情報群を生成し、生成した不正発行識別子情報群を監査結果出力部1215へ出力する。

[0301] 一時的に記憶している発行識別子情報が存在しないと判断する場合には、発行公開鍵確認部1213は、全ての公開鍵の正当性が確認されたことを示す旨の正当メッセージを監査結果出力部1215へ出力する。

(5)受付部1214

受付部1214は、ユーザの操作により、監査を開始する指示と、監査対象の鍵発行サーバのサーバ識別子とを受け付けると、監査開始命令と、サーバ識別子を制御部1212へ出力する。

[0302] (6)監査結果出力部1215

監査結果出力部1215は、発行公開鍵確認部1213から不正発行識別子情報群を受け取ると、受け取った不正発行識別子情報群をモニタ1250へ出力する。

監査結果出力部1215は、発行公開鍵確認部1213から正当メッセージを受け取ると、受け取った正当メッセージをモニタ1250へ出力する。

[0303] なお、モニタ1250では、監査結果出力部1215より受け取った情報を表示する。

(7)受信部1216

受信部1216は、鍵発行サーバ1100より、1以上の発行済鍵情報と、サーバ識別子とを受信すると、受信した1以上の発行済鍵情報と、サーバ識別子とを制御部1212へ出力する。

[0304] (8)送信部1217

送信部1217は、制御部1212より、発行済鍵依頼情報を受け取ると、受け取った発行済鍵依頼情報を鍵発行サーバ1100へ送信する。

2.4 端末装置1300の構成

端末装置1300は、第1の実施の形態における端末装置300と同様であるため、説明は省略する。

[0305] なお、端末装置1301、・・・、1302、1303、・・・、1304、1305、・・・、1306についても、端末装置300と同様であるため、説明は省略する。

2.5 鍵発行システム2の動作

ここでは、鍵発行システム2の動作について説明する。

(1)鍵発行システム2の動作概要

ここでは、鍵発行システム2の動作概要を説明する。

[0306] 以下では、鍵発行サーバ1100が端末装置1300に鍵を発行するときの動作概要を示す。

以降の説明において、1以上の発行済鍵情報を発行済鍵情報群として、記述する。

＜鍵発行時の動作概要＞

鍵発行時の動作概要を図31に示す流れ図を用いて、説明する。

[0307] 端末装置1300は、ユーザの操作により、鍵発行要求の指示を受け付けると、鍵発行依頼情報と、端末識別子「TID」とを、鍵発行サーバ100へ送信する(ステップS1000)。

鍵発行サーバ1100は、鍵発行依頼情報と、端末識別子「TID」とを、端末装置1300より受信すると、鍵発行処理にて秘密鍵及び公開鍵を生成し(ステップS1005)、証明書発行処理により、ステップS1005にて生成した公開鍵に対する公開鍵証明書を発行し、発行した公開鍵証明書と、ステップS1005にて生成した秘密鍵とを、端末装置1300へ送信する(ステップS1010)

端末装置1300は、鍵発行サーバ1100より、秘密鍵「SK」及び公開鍵証明書「Cert」を受信すると、受信した秘密鍵「SK」、及び公開鍵証明書「Cert」を記憶する(ステップS1015)。

[0308] <鍵の監査時の動作概要>

鍵の監査時の動作概要を図32に示す流れ図を用いて、説明する。

鍵発行監査サーバ1200は、監査処理にて、発行済鍵依頼情報を鍵発行サーバ1100へ送信する(ステップS1050)。

鍵発行サーバ1100は、鍵情報取得処理にて取得した発行済鍵情報群と、サーバ識別子とを鍵発行監査サーバ1200へ送信する(ステップS1055)。

[0309] (2)鍵発行処理

ここでは、図31に示す鍵発行処理の動作について、第1の実施の形態にて示す鍵発行処理との異なる点のみを、図11、図12、図13及び図14に示す流れ図を用いて、説明する。

本実施の形態に係る鍵発行処理は、図11、図12及び図13に示すステップS200からステップS325まで実行する。

[0310] 本実施の形態に係る鍵発行処理は、図13に示すステップS330を、鍵生成部1118は、組「SK=(p1、p2、d)」を秘密鍵として、秘密鍵格納部1111の秘密鍵格納領域へ書き込み、公開鍵証明書の生成命令を、証明書生成部1122へ出力するように変更する。

本実施の形態に係る鍵発行処理は、変更後のステップS330を実行すると、処理を

終了する。

[0311] (3)証明書発行処理

ここでは、図31に示す鍵発行処理の動作について、図33に示す流れ図を用いて、説明する。

証明書生成部1122は、鍵生成部1118より公開鍵証明書の生成命令を受け取ると、証明書用秘密鍵格納部より証明書用秘密鍵「C__SK」を、公開鍵格納部1112より公開鍵「PK」を、識別子格納部1110より発行識別子情報「IDI」を、それぞれ読み出す(ステップS1100)。

[0312] 証明書生成部1122は、読み出した秘密鍵「C__SK」、公開鍵「PK」及び発行識別子情報「IDI」を用いて、公開鍵証明書「Cert」を生成し、生成した公開鍵証明書「Cert」を証明書格納部1113へ書き込み、公開鍵証明書「Cert」の配布開始命令を情報取得部1119へ出力する(ステップS1105)。

情報取得部1119は、証明書生成部1122から配布開始命令を受け取ると、秘密鍵格納部1111にて記憶している秘密鍵「SK」と、証明書格納部1113にて記憶している公開鍵証明書「Cert」と、制御部1114の端末情報記憶領域にて記憶している端末識別子とを、それぞれ読み出し、読み出した秘密鍵「SK」及び公開鍵証明書「Cert」を、読み出した端末識別子に対応する端末装置1300へ送信部1121を介して送信する(ステップS1110)。

[0313] 情報取得部1119は、公開鍵格納部1112より発行した公開鍵「PK=(n、e)」を、識別子格納部1110より発行した発行識別子情報「IDI」を、それぞれ読み出し、読み出した公開鍵「PK」及び発行識別子情報「IDI」を1つの組として、発行済鍵情報格納部1124へ書き込む(ステップS1115)。

(4)鍵情報取得処理

ここでは、図32に示す鍵情報取得処理の動作について、図34に示す流れ図を用いて、説明する。

[0314] 鍵発行サーバ1100の制御部1114は、鍵発行監査サーバ1200から受信部1120を介して、発行済鍵依頼情報を受け取ると、鍵情報取得命令を情報取得部1119へ出力する(ステップS1200)。

鍵発行サーバ1100の情報取得部1119は、制御部1114から鍵情報取得命令を受け取ると、発行済鍵情報格納部1124より、全ての発行済鍵情報を読み出す(ステップS1205)。

[0315] 情報取得部1119は、制御部1114のサーバ識別子記憶領域1130よりサーバ識別子を読み出し、読み出した発行済鍵情報群とサーバ識別子とを、送信部1121を介して鍵発行監査サーバ1200へ送信する(ステップS1210)。

(5)監査処理

ここでは、図32に示す監査処理の動作について、図35に示す流れ図を用いて、説明する。

[0316] 鍵発行監査サーバ1200の受付部1214は、ユーザの操作により、監査を開始する指示と、監査対象の鍵発行サーバのサーバ識別子とを受け付けると、監査開始命令と、サーバ識別子を制御部1212へ出力する(ステップS1300)。

制御部1212は、受付部1214より、公開鍵の監査を開始する監査開始命令と、監査対象のサーバ識別子(ここでは、「SID」とする。)を受け付けると、発行済鍵依頼情報を、送信部1217を介してサーバ識別子に対応する鍵発行サーバ1100へ送信する(ステップS1305)。

[0317] 制御部1212は、受付部1214より受け取ったサーバ識別子をサーバ情報記憶領域1220へ書き込む(ステップS1310)。

制御部1212は、鍵発行サーバ1100から受信部217を介して、1以上の発行済鍵情報とサーバ識別子とを受け取る(ステップS1315)。

制御部1212は、受け取ったサーバ識別子と、サーバ情報記憶領域にて記憶しているサーバ識別子とが一致するか否かを判断する(ステップS1320)。

[0318] 一致すると判断する場合には(ステップS1320における「YES」)、制御部1212は、受け取った1以上の発行済鍵情報を発行済鍵情報格納部1211へ書き込み、監査開始命令と受け取ったサーバ識別子とを発行公開鍵確認部1213へ出力する(ステップS1325)。

発行公開鍵確認部1213は、確認処理において、公開鍵の正当性の確認を行い、結果をモニタ1250にて表示する。

[0319] 一致しないと判断する場合には(ステップS1320における「NO」)、制御部1212は、処理を終了する。

(6)確認処理

ここでは、図35に示す確認処理の動作について、図36に示す流れ図を用いて、説明する。

[0320] 発行公開鍵確認部1213は、制御部1212より監査開始命令とサーバ識別子とを受け取ると、受け取ったサーバ識別子を用いて、対応する第1検証値「c11」及び第2検証値「c12」を、確認情報格納部1210から読み出す(ステップS1400)。

発行公開鍵確認部1213は、発行済鍵情報格納部1211から、未読の発行済鍵情報を1つ読み出す(ステップS1405)。

[0321] 発行公開鍵確認部1213は、読み出した発行済鍵情報に含まれる公開鍵「PK」と発行識別子情報「IDI」と、第1検証値「c11」及び第2検証値「c12」とを用いて、公開鍵「PK」が、発行識別子情報「IDI」を用いて生成されたか否かを確認する(ステップS1410)。なお、確認方法は、第1の実施の形態と同様であるため、説明は省略する。

[0322] 発行公開鍵確認部1213は、「n−(c11×c12)」が、「IDI」で割り切れないと判断する場合、つまり公開鍵が不正であると判断する場合(ステップS1410における「NO」)、読み出した発行識別子情報「IDI」を一時的に記憶する(ステップS1415)。

発行公開鍵確認部1213は、「n−(c11×c12)」が、「IDI」で割り切れると判断する場合、つまり公開鍵が正当であると判断する場合には(ステップS1410における「YES」)、ステップS1415を省略する。

[0323] 発行公開鍵確認部1213は、未読の発行済鍵情報が存在するか否かを判断し(ステップS1420)、未読の発行済鍵情報が存在すると判断する場合には(ステップS1420における「YES」)、ステップS1405へ戻る。

未読の発行済鍵情報が存在しないと判断する場合には(ステップS1420における「NO」)、一時的に記憶している発行識別子情報が存在するか否かを判断する(ステップS1425)。

[0324] 一時的に記憶している発行識別子情報が存在すると判断する場合には(ステップS

1425における「YES」)、発行公開鍵確認部1213は、記憶されている全ての発行識別子を連結し、不正発行識別子情報群を生成し、生成した不正発行識別子情報群を、監査結果出力部1215を介して、モニタ1250にて表示する(ステップS1430)。

一時的に記憶している発行識別子情報が存在しないと判断する場合には(ステップS1425における「NO」)、発行公開鍵確認部1213は、全ての公開鍵の正当性が確認されたことを示す旨の正当メッセージを、監査結果出力部1215を介して、モニタ1250にて表示する(ステップS1435)。

[0325] 3. まとめ

上記の第1の実施の形態にて示す鍵発行サーバ100の素数生成部116の素数情報生成部133は、図37に示す動作を繰り返すことにより、8ビットの素数から512ビットの素数を生成する。

素数情報生成部133は、8ビットの素数から16ビットの素数を生成し(ステップS1700)、生成した16ビットの素数から32ビットの素数を生成し(ステップS1705)、以降順に、32ビットの素数から64ビットの素数、64ビットの素数から128ビットの素数、128ビットの素数から256ビットの素数を生成し(ステップS1710、S1715、及びS1720)、最後に、生成した256ビットの素数から516ビットの素数を生成する(ステップS1725)。

[0326] 素数生成部116は、8ビットから128ビットの素数を生成する間は、制御情報「情報C」により、従来と同様の生成方法にて、素数を生成する。

素数生成部116は、ステップS1720においては、制御情報「情報B」により、生成される素数が、発行識別子情報「IDI」に対して一意となるように、単射の関数「f」を用いて256ビットの素数を生成する。

[0327] 素数生成部116は、ステップS1725においては、制御情報「情報A」により、生成される素数の正当性を確認できるように、発行識別子情報「IDI」を埋め込んだ512ビットの素数を生成する。

これにより、鍵発行サーバ100は、単射関数「f」を用いることにより、端末装置毎に異なる秘密鍵及び公開鍵を生成することができる。また、鍵発行サーバ100にて、256ビットの素数から512ビットの素数を生成する際に、生成される素数に、発行識別子

情報「IDI」が埋め込まれているため、証明書発行サーバ200は、生成された公開鍵と発行識別子情報とを用いて、公開鍵の正当性を確認することができる。

[0328] なお、第2の実施の形態においても、上記の記載と同様に、鍵発行サーバ1100は、単射関数「f」を用いることにより、端末装置毎に異なる秘密鍵及び公開鍵を生成することができる。また、鍵発行サーバ1100にて、256ビットの素数から512ビットの素数を生成する際に、生成される素数に、発行識別子情報「IDI」が埋め込まれているため、鍵発行監査サーバ1200は、生成された公開鍵と発行識別子情報とを用いて、公開鍵の正当性を確認することができる。

[0329] 上記第1の実施の形態によると、鍵発行サーバ100は、単射の関数「f」を用いることにより、複数回素数生成を行っても、素数が一致しないことを比較することなく、証明できる素数を生成することが実現できる。

上記第1の実施の形態によると、鍵発行サーバ100が、生成する素数に発行識別子情報「IDI」を埋め込むことにより、証明書発行サーバ200は、正しく鍵発行しているかを発行識別子情報「IDI」で割り切れるかをチェックすることで確認できる。

[0330] 従来、1台の鍵発行サーバを有する鍵発行システムがある。しかしながら、ユーザが増加すると、素数を生成する際に、複数回べき乗を行うことにより計算量が大きくなるため、計算時間が大きくなってくる。そこで、鍵発行サーバを複数もち、それぞれで鍵発行をすることにより、計算量の分散を図ることがある。しかしながら、複数台の鍵発行サーバをもつ従来の鍵発行システムでは、例えば、2人のユーザで同じ素数が鍵となる場合がある。このとき、暗号の安全性が著しく低下する。なぜなら、例えば、ユーザAの素数をpA1、pA2とし、nA＝pA1×pA2、ユーザBの素数をpB1、pB2とし、nB＝pB1×pB2とする。このとき、pA1＝pB1であれば、ユーザAはGCD(pA1, nB)を求めることにより、ユーザBの素数の一つがpA1と等しいことがわかり、その結果、nB／pA1を計算することにより、pB2も得ることができる。RSA暗号は、素因数分解を安全性の根拠としているため、素因数が判明すると、簡単に解読可能になる。そのため、ユーザAはユーザBの公開鍵で暗号化した暗号文を解ける。また、同様に、ユーザBはユーザAの公開鍵で暗号化した暗号文を解けてしまう。

[0331] 従来技術では、複数回素数生成を行ったときに素数が一致する可能性があり、そ

れにより、暗号の安全性を著しく低下させる。それに対しては、発行済の素数(秘密鍵)と発行した素数を比較することにより、一致しないことを確認できる。しかし、通常の公開鍵暗号のシステムでは、発行した後の公開鍵は鍵発行サーバで管理するが、秘密鍵は機密性が高いため、削除してしまうことが多い。そのため、新たに発行済の素数(秘密鍵)を管理する必要がある。さらに、発行数が10億個程度に大きさになると、比較する時間が大きく現実的でない。

[0332] また、複数の鍵発行サーバで発行した場合、すべての鍵発行サーバで発行した素数が一致させないため、各鍵発行サーバ間で、発行した素数、すなわち、秘密鍵を互いにチェックさせる必要がある。各鍵発行サーバ間で信頼関係がある場合は問題ないが、各鍵発行サーバはそれぞれ別の会社が設置することが多いため、信頼できるとは限らない。さらに、もし、各鍵発行サーバ間で信頼関係がある場合であっても、鍵を発行するたびに、各鍵発行サーバの秘密鍵のデータベースにアクセスするため、各鍵発行サーバ間の通信量が大きくなる。このように各鍵発行サーバ間で互いにチェックすることも現実的でない。

[0333] 本発明の鍵発行サーバを用いると、素数の生成を複数回行っても、素数が一致しないことを比較することなく、証明できる。

3.1 変形例

本発明を上記の第1、第2実施の形態及び素数生成の変形例1、2、3に基づいて説明してきたが、本発明は、上記の実施の形態に限定されないのはもちろんである。以下のような場合も本発明に含まれる。

[0334] (1)発行識別子情報「IDI」は、サーバ識別子、端末識別子及び数「1」の連結からなるとしたが、これに限定されない。IDIはサーバ識別子と、カウンタにより生成される発行識別子「PID」とを用いて生成してもよい。ここで、発行識別子「PID」は、1から発行順に割り当てられた奇数である。このとき、識別子生成部115は、素数を発行(生成)するたびに、数「2」をインクリメントしていくことで、容易に毎回異なる素数を生成できることになる。

[0335] (2)128ビットから256ビットの素数を生成する際に、単射関数を用いたが、これに限定されない。発行識別子情報を埋め込む前であれば、単射関数を施す動作は、ど

の段階でもよい。

例えば、8ビットの素数から16ビットの素数を生成する際に、単射関数を施してもよい。または、16ビットの素数から32ビットの素数を生成する際に、単射関数を施してもよい。または、32ビットの素数から64ビットの素数を生成する際に、単射関数を施してもよい。または、64ビットの素数から128ビットの素数を生成する際に、単射関数を施してもよい。

[0336] ただし、発行識別子「IDI」のビット数は、入力の用いられる素数「q」のビット数よりも小さく、乱数「R1」のビット数は、(lenq−lenIDI−1)ビットであり、数「R」のビット数は、(lenq−1)ビットである。

(3)第1の実施の形態における素数生成部116を、1つの素数生成装置としてもよい。このとき、素数生成装置は、発行識別子情報「IDI」とそのビットサイズ「lenIDI」が与えられた場合、与えられた「IDI」及びそのビットサイズ「lenIDI」と、予め記憶されている8ビットの素数とから、512ビットの素数を生成する。

[0337] また、第2の実施の形態における素数生成部1116も同様に、1つの素数生成装置としてもよい。

(4)第1の実施の形態における素数生成部116を、予め記憶している8ビットの素数から128ビットの素数を生成する第1素数生成部と、128ビットの素数から512ビットの素数を生成する第2素数生成部とからなるとしてもよい。また、第1素数生成部及び第2素数生成部を、それぞれ個別の素数生成装置としてもよい。

[0338] 第1素数生成部は、従来と同様の方法にて、8ビットの素数から128ビットの素数を生成する。従来の方法については、特許文献1及び非特許文献3が詳しい。

以下に、第2素数生成部の構成の一例を、図38に示す。ここでは、第2素数生成部を1つの素数生成装置2100として説明する。素数生成装置2100は、素数「q1」と、そのビットサイズ「lenq1」(ここでは、ビットサイズを128ビットとする。)と、発行識別子情報「IDI」と、そのビットサイズ「lenIDI」とが与えられた場合に、(4×lenq1)ビットからなる素数「N」を出力する。なお、ここで示す素数生成装置2100は、第1の実施の形態にて示す第1及び第2検証値を用いないで、素数「N」を生成する。

[0339] 素数生成装置2100は、図38に示すように、受付部2101、受付情報記憶部2102

、素数シード生成部2103、乱数生成部2104、素数候補生成部2105、第1素数判定部2106及び第2素数判定部2107から構成されている。

素数生成装置2100は、具体的には、マイクロプロセッサ、ROM、RAM、ハードディスクユニット、ディスプレイユニット、キーボード、マウスなどから構成されるコンピュータシステムである。前記RAM又は前記ハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することにより、素数生成装置2100は、その機能を達成する。

[0340] ＜受付情報記憶部2102＞

受付情報記憶部2102は、素数「N」を生成する際に与えられた素数「q1」、素数「q1」のビットサイズ「lenq1」、発行識別子情報「IDI」及び発行識別子情報のビットサイズ「lenIDI」を記憶する領域を備えている。

＜受付部2101＞

受付部2101は、素数「q1」、素数「q1」のビットサイズ「lenq1（例えば、128ビット）」、発行識別子情報「IDI」及び発行識別子情報のビットサイズ「lenIDI」を、外部（例えば、上記に示す第1素数生成部）より受け付け、受け付けた素数「q1」、そのビットサイズ「lenq1」、発行識別子情報「IDI」及びそのビットサイズ「lenIDI」を受付情報記憶部2102へ書き込む。

[0341] 受付部2101は、受け付けた各情報を、素数シード生成部2103へ出力する。

＜素数シード生成部2103＞

素数シード生成部2103は、上記第1の実施の形態にて示す素数生成部116において、制御情報装が「情報B」の場合に行う動作と同様の動作を行うので、ここでの説明は省略する。なお、ここでは、128ビットの素数「q1」から256ビットの素数「q2」を生成するものとする。

[0342] 素数シード生成部2103、生成した素数「q2」を素数候補生成部2105へ出力する。

＜乱数生成部2104＞

乱数生成部2104は、第1生成指示を、素数候補生成部2105から受け取ると、素数「q1」のビットサイズ「lenq1」と、発行識別子情報「IDI」のビットサイズ「lenIDI」とを

、受付情報記憶部2102より読み出す。

[0343] 乱数生成部2104は、読み出したビットサイズ「lenq1」及び「lenIDI」を用いて、(2×lenq1−lenIDI−1)ビットの乱数「R1」を生成する。ここで、乱数「R1」の最上位ビットは1とする。

乱数生成部2104は、生成した乱数「R1」を素数候補生成部2105へ出力する。

また、乱数生成部2104は、第1素数判定部2106及び第2素数判定部2107の何れかから、再度乱数を生成する旨の第2生成指示を受け付けると、各ビットサイズを読み出し、上記の動作を行う。

[0344] ＜素数候補生成部2105＞

素数候補生成部2105は、生成された数を記憶する生成情報記憶領域とを有している。

素数候補生成部2105は、素数シード生成部2103より素数「q2」を受け取ると、第1生成指示を乱数生成部2104へ出力する。

[0345] 素数候補生成部2105は、乱数生成部2104より、乱数「R1」を受け取ると、受付情報記憶部2102にて記憶している発行識別子情報「IDI」を読み出す。

素数候補生成部2105は、素数シード生成部2103より受け取った素数「q2」、受付情報記憶部2102より読み出した発行識別子情報「IDI」及び乱数生成部2104より受け取った乱数「R1」とを用いて、数「R＝IDI×R1」と、数「N＝2×R×q2＋1」とを生成する。

[0346] 素数候補生成部2105は、素数「q1」のビットサイズ「lenq1」を、受付情報記憶部2102より読み出し、生成した数「N」のビットサイズが「4×lenq1」であるか否かを判断する。

「4×lenq1」であると判断する場合には、素数候補生成部2105は、生成した数「N」を第1素数判定部2106へ出力し、生成した数「R」を生成情報記憶領域に記憶する。

[0347] 「4×lenq1」でないと判断する場合には、素数候補生成部2105は、乱数生成部2104より受け取った乱数「R1」に2を掛けて、その結果を「R1」として、再度、上記の動作を行い、数「R」及び「N」を生成する。

素数候補生成部2105は、数「N」のビットサイズが、「4×lenq1」となるまで、上記の動作を繰り返す。

[0348] ＜第1素数判定部2106＞

第1素数判定部2106は、第1の実施の形態にて示す第1素数判定部143と同様の動作であるため、ここでの説明は省略する。

＜第2素数判定部2107＞

第2素数判定部2107は、第1の実施の形態にて示す第2素数判定部144と同様の動作であるため、ここでの説明は省略する。

[0349] なお、第2素数判定部2107は、判定により、生成した数「N」が素数であると判断する場合には、生成した数「N」を素数「N」として出力する。

＜素数生成装置2100の動作＞

以下に、素数生成装置2100の動作について説明する。

(素数生成処理)

ここでは、素数生成装置2100にて行われる素数生成処理について、図39に示す流れ図を用いて、説明する。

[0350] 素数生成装置2100は、受付部2101において、素数「q1」、素数「q1」のビットサイズ「lenq1」、発行識別子情報「IDI」及び発行識別子情報のビットサイズ「lenIDI」を受け付け、受け付けた各情報を受付情報記憶部2102へ書き込む(ステップS2000)。

素数生成装置2100は、素数シード生成部2103において、ステップS2000にて受け付けた各情報を用いて、素数「q2」を生成する(ステップS2005)。

[0351] 素数生成装置2100は、乱数生成部2104において、ステップS2000にて受け付けたビットサイズ「lenq1」及び「lenIDI」を用いて、(2×lenq1−lenIDI−1)ビットの乱数「R1」を生成する(ステップS2010)。ここで、乱数「R1」の最上位ビットは1とする。

素数生成装置2100は、素数候補生成部2105において、ステップS2000にて受け付けられた発行識別子情報「IDI」、ステップS2005にて生成された素数「q2」及びステップS2010にて生成された乱数「R1」とを用いて、素数候補生成処理を施すことにより、数「R」及び「N」を生成する(ステップS2015)。素数生成装置2100は、第1

素数判定部2106において、ステップS2015にて生成した数「N」を用いて、上記に示す式(eq1)が成立するか否かを判定する(ステップS2020)。

[0352] 式(eq1)が成立していると判断する場合には(ステップS2020における「YES」)、素数生成装置2100は、第2素数判定部2107において、ステップS2015にて生成した数「R」と「N」とを用いて、上記に示す式(eq2)が成立するか否かを判定する(ステップS2025)。

式(eq2)が成立していると判断する場合には(ステップS2025における「YES」)、素数生成装置2100は、数「N」を素数「N」として出力し、処理を終了する(ステップS2030)。

[0353] 式(eq1)が成立していないと判断する場合(ステップS2020における「NO」)、及び式(eq2)が成立していないと判断する場合には(ステップS2025における「NO」)、ステップS2010に戻り、再度処理を行う。

(素数候補生成処理)

ここでは、素数生成処理のステップS2015にて行われる素数候補生成処理について、図40に示す流れ図を用いて説明する。

[0354] 素数候補生成部2105は、素数生成処理のステップS2000にて受け付けた発行識別子情報「IDI」と、ステップS2010にて生成した乱数「R1」とを用いて、数「R」を生成する(ステップS2050)。ここで、数「R」は「R=IDI×R1」である。

素数候補生成部2105は、素数生成処理のステップS2005にて生成された素数「q2」と、ステップS2050にて生成された数「R」とを用いて、数「N」を生成する(ステップS2055)。ここで、数「N」は、「N=2×R×q2+1」である。

[0355] 素数候補生成部2105は、生成した数「N」のビットサイズが「4×lenq1」であるか否かを判断する(ステップS2060)。

「4×lenq1」であると判断する場合には(ステップS2060における「YES」)、処理を終了する。「4×lenq1」でないと判断する場合には(ステップS2060における「NO」)、素数生成処理のステップS2010にて生成した乱数「R1」に2を掛けて、その結果を「R1」として、ステップS2050へ戻る(ステップS2065)。

[0356] <その他>

ここでは、生成する秘密鍵である素数のビットサイズは512ビットとしているが、これに限定されない。1024ビットであっても、2048ビットであってもよい。また、上記の第1素数生成部で生成する素数も同様に128ビットに限らない。

(5)上記に示す素数シード生成部2103を1つの素数生成装置としてもよい。以下に、この場合の素数生成装置2200について、説明する。素数生成装置2200は、素数「q」と、そのビットサイズ「lenq」(ここでは、ビットサイズを128ビットとする。)と、発行識別子情報「IDI」と、そのビットサイズ「lenIDI」とが与えられた場合に、(2×lenq)ビットからなる素数「N」を出力する。

[0357] 素数生成装置2200は、図41に示すように、受付部2201、受付情報記憶部2202、乱数生成部2203、素数候補生成部2204、第1素数判定部2205及び第2素数判定部2206から構成されている。

素数生成装置2200は、具体的には、マイクロプロセッサ、ROM、RAM、ハードディスクユニット、ディスプレイユニット、キーボード、マウスなどから構成されるコンピュータシステムである。前記RAM又は前記ハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することにより、素数生成装置2200は、その機能を達成する。

[0358] <受付情報記憶部2202>

受付情報記憶部2202は、素数「N」を生成する際に与えられた素数「q」、素数「q」のビットサイズ「lenq」、発行識別子情報「IDI」及び発行識別子情報のビットサイズ「lenIDI」を記憶する領域を備えている。

<受付部2201>

受付部2201は、素数「q」、素数「q」のビットサイズ「lenq」、発行識別子情報「IDI」及び発行識別子情報のビットサイズ「lenIDI」を、外部(例えば、上記に示す第1素数生成部)より受け付け、受付部2201は、受け付けた素数「q」、そのビットサイズ「lenq」、発行識別子情報「IDI」及びそのビットサイズ「lenIDI」を受付情報記憶部2202へ書き込む。

[0359] 受付部2201は、処理を開始する旨の開始指示を素数候補生成部2204へ出力する。

＜乱数生成部2203＞

乱数生成部2203は、乱数を生成する旨の第1生成指示を、素数候補生成部2204から受け取ると、素数「q」のビットサイズ「lenq」と、発行識別子情報「IDI」のビットサイズ「lenIDI」とを受付情報記憶部2202より読み出す。

[0360] 乱数生成部2203は、読み出したビットサイズ「lenq」及び「lenIDI」を用いて、(lenq−lenIDI−1)ビットの乱数「R1」を生成する。ここで、乱数「R1」の最上位ビットは1とする。乱数生成方法は、非特許文献2が詳しい。

乱数生成部2203は、生成した乱数「R1」を素数候補生成部2204へ出力する。

また、乱数生成部2203は、第1素数判定部2205及び第2素数判定部2206の何れかから、再度乱数を生成する旨の第2生成指示を受け付けると、各ビットサイズを読み出し、上記の動作を行う。

[0361] ＜素数候補生成部2204＞

素数候補生成部2204は、単射である関数「f」を予め記憶している関数記憶領域と、関数「f」を用いて生成された数を記憶する生成情報記憶領域とを有している。

素数候補生成部2204は、受付部2201より開始指示を受け取ると、第1生成指示を乱数生成部2203へ出力する。

[0362] 素数候補生成部2204は、乱数「R1」を乱数生成部2203より受け取ると、受付情報記憶部2202にて記憶している素数「q」及び発行識別子情報「IDI」を読み出す。

素数候補生成部2204は、関数記憶領域にて記憶している関数「f」と、読み出した素数「q」及び発行識別子情報「IDI」と、乱数生成部2203より受け取った乱数「R1」とを用いて、数「R＝f(IDI｜｜R1)」と、数「N＝2×R×q＋1」とを生成する。

[0363] 素数候補生成部2204は、生成した数「N」のビットサイズが「2×lenq」であるか否かを判断する。

「2×lenq」であると判断する場合には、素数候補生成部2204は、生成した数「N」を第1素数判定部2205へ出力し、生成した数「R」を生成情報記憶領域に記憶する。

[0364] 「2×lenq」でないと判断する場合には、素数候補生成部2204は、乱数生成部2203より受け取った乱数「R1」に2を掛けて、その結果を「R1」として、再度、上記の動

作を行い、上記の式を満たす数「R」及び「N」を生成する。

素数候補生成部2204は、生成した数「N」のビットサイズが、「2×lenq」となるまで、上記の動作を繰り返す。

[0365] ＜第1素数判定部2205＞

第1素数判定部2205は、第1の実施の形態にて示す第1素数判定部143と同様の動作であるため、ここでの説明は省略する。

＜第2素数判定部2206＞

第2素数判定部2206は、第1の実施の形態にて示す第2素数判定部144と同様の動作であるため、ここでの説明は省略する。

[0366] なお、第2素数判定部2206は、判定により、生成した数「N」が素数であると判断する場合には、生成した数「N」を素数「N」として出力する。

＜素数生成装置2200の動作＞

以下に、素数生成装置2200の動作について説明する。

（素数生成処理）

ここでは、素数生成装置2200にて行われる素数生成処理について、図39に示す流れ図を用いて、変更点のみ説明する。

[0367] 素数生成装置2200は、ステップS2000において、素数「q」、素数「q」のビットサイズ「lenq」、発行識別子情報「IDI」及び発行識別子情報のビットサイズ「lenIDI」を、ユーザ操作により受け付け、受け付けた各情報を受付情報記憶部2202へ書き込むように変更する。

素数生成装置2200は、上記のように変更されたステップS2000の実行後、ステップS2005を省略し、以下のように変更されたステップS2010を実行する。素数生成装置2200は、ステップS2010において、(lenq−lenIDI−1)ビットの乱数「R1」を生成するように変更する。

[0368] 以降の動作の流れは、図39と同様であるため、説明は省略する。

（素数候補生成処理）

ここでは、素数候補生成処理について、図40に示す流れ図を用いて、変更点のみ説明する。

先ず、ステップS2050を、数「R＝f(IDI｜｜R1)」を生成するように変更する。

[0369] 次に、ステップS2055を、数「N＝2×R×q＋1」を生成するように変更する。

以降の動作の流れは、図40と同様であるため、説明は省略する。

(6)素数生成変形例3における素数生成部116Cを、予め記憶している8ビットの素数から256ビットの素数を生成する第1素数生成部と、256ビットの素数から512ビットの素数を生成する第2素数生成部とからなるとしてもよい。また、第1素数生成部及び第2素数生成部を、それぞれ個別の素数生成装置としてもよい。

[0370] 第1素数生成部は、従来と同様の方法にて、8ビットの素数から256ビットの素数を生成する。

以下に、第2素数生成部の構成の一例を、図42に示す。ここでは、第2素数生成部を1つの素数生成装置2300として説明する。素数生成装置2300は、素数「q」と、そのビットサイズ「lenq」(ここでは、ビットサイズを128ビットとする。)と、発行識別子情報「IDI」と、そのビットサイズ「lenIDI」とが与えられた場合に、(2×lenq)ビットからなる素数「N」を出力する。なお、ここで示す素数生成装置2300は、第1の実施の形態にて示す第1及び第2検証値を用いないで、素数「N」を生成する。

[0371] 素数生成装置2300は、図42にて示すように、受付部2301、受付情報記憶部2302、識別子素数生成部2303、乱数生成部2304、素数候補生成部2305、第1素数判定部2306及び第2素数判定部2307から構成されている。

素数生成装置2300は、具体的には、マイクロプロセッサ、ROM、RAM、ハードディスクユニット、ディスプレイユニット、キーボード、マウスなどから構成されるコンピュータシステムである。前記RAM又は前記ハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することにより、素数生成装置2300は、その機能を達成する。

[0372] ＜受付情報記憶部2302＞

受付情報記憶部2302は、素数「N」を生成する際に与えられた素数「q」、素数「q」のビットサイズ「lenq」、発行識別子情報「IDI」及び発行識別子情報のビットサイズ「lenIDI」を記憶する領域を備えている。

＜受付部2301＞

受付部2301は、素数「q」、素数「q」のビットサイズ「lenq」、発行識別子情報「IDI」及び発行識別子情報のビットサイズ「lenIDI」を、外部（例えば、第1の素数生成部）より受け付け、受け付けた素数「q」、そのビットサイズ「lenq」、発行識別子情報「IDI」及びそのビットサイズ「lenIDI」を受付情報記憶部2302へ書き込む。

[0373] 受付部2301は、処理を開始する旨の開始指示を、識別子素数生成部2303へ出力する。

＜識別子素数生成部2303＞

識別子素数生成部2303は、素数「qg」及びそのビットサイズ「lenqg」を予め記憶している。

[0374] 識別子素数生成部2303は、発行識別子「IDI」と素数「qg」から一意的に素数を生成する素数生成関数「gp」と、単射の関数「f」とを予め記憶している。

識別子素数生成部2303は、受付部2301より開始指示を受け取ると、発行識別子情報「IDI」を、受付情報記憶部2302より読み出す。

識別子素数生成部2303は、予め記憶している素数「qg」及び素数生成関数「gp」と、読み出した発行識別子情報「IDI」より、素数「pIDI＝gp(IDI, qg)」を生成する。素数「pIDI」の生成方法は、素数生成の変形例3にて示す方法と同様であるため、説明は省略する。

[0375] 識別子素数生成部2303は、生成した素数「pIDI」を素数候補生成部2305へ出力する。

＜乱数生成部2304＞

乱数生成部2304は、第1生成指示を、素数候補生成部2305から受け取ると、素数「q」のビットサイズ「lenq」を、受付情報記憶部2302より読み出し、素数「qg」のビットサイズ「lenqg」を識別子素数生成部2303より読み出す。

[0376] 乱数生成部2304は、読み出したビットサイズ「lenq」及び「lenqg」を用いて、(lenq−2×lenqg−1)ビットの乱数「R」を生成する。ここで、乱数「R」の最上位ビットは1とする。

乱数生成部2304は、生成した乱数「R」を素数候補生成部2305へ出力する。

また、乱数生成部2304は、第1素数判定部2306及び第2素数判定部2307の何

れかから、再度乱数を生成する旨の第2生成指示を受け付けると、各ビットサイズを読み出し、上記の動作を行う。

[0377] ＜素数候補生成部2305＞

素数候補生成部2305は、識別子素数生成部2303より素数「pIDI」を受け取ると、第1生成指示を乱数生成部2304へ出力する。

素数候補生成部2305は、乱数生成部2304より、乱数「R」を受け取ると、受付情報記憶部2302にて記憶している素数「q」を読み出す。

[0378] 素数候補生成部2305は、識別子素数生成部2303より受け取った素数「pIDI」、受付情報記憶部2302より読み出した素数「q」及び乱数生成部2304より受け取った乱数「R」とを用いて、「N＝2×R×q×pIDI＋1」を生成する。

素数候補生成部2305は、素数「q」のビットサイズ「lenq」を、受付情報記憶部2302より読み出し、生成した数「N」のビットサイズが「2×lenq」であるか否かを判断する。

[0379] 「2×lenq」であると判断する場合には、素数候補生成部2305は、生成した数「N」を第1素数判定部2306へ出力し、乱数「R」を一時的に記憶する。

「2×lenq」でないと判断する場合には、素数候補生成部2305は、乱数生成部2304より受け取った乱数「R」に2を掛けて、その結果を「R」として、再度、上記の動作を行い、数「N」を生成する。

[0380] 素数候補生成部2305は、数「N」のビットサイズが、「2×lenq」となるまで、上記の動作を繰り返す。

＜第1素数判定部2306＞

第1素数判定部2306は、第1の実施の形態にて示す第1素数判定部143と同様の動作であるため、ここでの説明は省略する。

[0381] ＜第2素数判定部2307＞

第2素数判定部2307は、第1の実施の形態にて示す第2素数判定部144と同様の動作であるため、ここでの説明は省略する。

なお、第2素数判定部2307は、判定により、生成した数「N」が素数であると判断する場合には、生成した数「N」を素数「N」として出力する。

[0382] ＜素数生成装置2300の動作＞

以下に、素数生成装置2300の動作について説明する。

(素数生成処理)

ここでは、素数生成装置2300にて行われる素数生成処理について、図39に示す流れ図を用いて、変更点のみ説明する。

[0383] 素数生成装置2300は、ステップS2000において、素数「q」、素数「q」のビットサイズ「lenq」、発行識別子情報「IDI」及び発行識別子情報のビットサイズ「lenIDI」を、ユーザ操作により受け付け、受け付けた各情報を受付情報記憶部2202へ書き込むように変更する。

素数生成装置2300は、ステップS2005において、素数「pIDI」を生成するように変更する。

[0384] 素数生成装置2300は、ステップS2010において、(lenq−2×lenqg−1)ビットの乱数「R」を生成するように変更する。

以降の動作の流れは、図39と同様であるため、説明は省略する。

(素数候補生成処理)

ここでは、素数候補生成処理について、図40に示す流れ図を用いて、変更点のみ説明する。

[0385] 先ず、ステップS2050を、省略する。

次に、ステップS2055を、数「N＝2×R×q×pIDI＋1」を生成するように変更する。

以降の動作の流れは、図40と同様であるため、説明は省略する。

＜その他＞

ここでは、生成する秘密鍵である素数のビットサイズは512ビットとしているが、これに限定されない。1024ビットであっても、2048ビットであってもよい。また、上記の第1素数生成部で生成する素数も同様に256ビットに限らない。

[0386] (7)第1の実施の形態における素数生成部116を、予め記憶している8ビットの素数から256ビットの素数を生成する第1素数生成部と、256ビットの素数から512ビットの素数を生成する第2素数生成部とからなるとしてもよい。また、第1素数生成部及

び第2素数生成部を、それぞれ個別の素数生成装置としてもよい。

第1素数生成部は、従来と同様の方法にて、8ビットの素数から128ビットの素数を生成し、上記に示す素数生成装置2200を適用して、128ビットの素数から256ビットの素数を生成する。

[0387] 以下に、第2素数生成部の構成の一例を、図43に示す。ここでは、第2素数生成部を1つの素数生成装置2400として説明する。素数生成装置2400は、素数「q」と、そのビットサイズ「lenq」(ここでは、ビットサイズを256ビットとする。)と、発行識別子情報「IDI」と、そのビットサイズ「lenIDI」とが与えられた場合に、(2×lenq)ビットからなる素数「N」を出力する。なお、ここで示す素数生成装置2400は、第1の実施の形態にて示す第1及び第2検証値を用いないで、素数「N」を生成する。

[0388] 素数生成装置2400は、図43に示すように、受付部2401、受付情報記憶部2402、乱数生成部2403、素数候補生成部2404、第1素数判定部2405及び第2素数判定部2406から構成されている。

素数生成装置2400は、具体的には、マイクロプロセッサ、ROM、RAM、ハードディスクユニット、ディスプレイユニット、キーボード、マウスなどから構成されるコンピュータシステムである。前記RAM又は前記ハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することにより、素数生成装置2400は、その機能を達成する。

[0389] ＜受付情報記憶部2402＞

受付情報記憶部2402は、素数「N」を生成する際に与えられた素数「q」、素数「q」のビットサイズ「lenq」、発行識別子情報「IDI」及び発行識別子情報のビットサイズ「lenIDI」を記憶する領域を備えている。

＜受付部2401＞

受付部2401は、素数「q」、素数「q」のビットサイズ「lenq」、発行識別子情報「IDI」及び発行識別子情報のビットサイズ「lenIDI」を、外部(例えば、上記に示す第1素数生成部)より受け付け、受付部2401は、受け付けた素数「q」、そのビットサイズ「lenq」、発行識別子情報「IDI」及びそのビットサイズ「lenIDI」を受付情報記憶部2402へ書き込む。

[0390] 受付部2401は、処理を開始する旨の開始指示を素数候補生成部2404へ出力する。

＜乱数生成部2403＞

乱数生成部2403は、乱数を生成する旨の第1生成指示を、素数候補生成部2404から受け取ると、素数「q」のビットサイズ「lenq」と、発行識別子情報「IDI」のビットサイズ「lenIDI」とを受付情報記憶部2402より読み出す。

[0391] 乱数生成部2403は、読み出したビットサイズ「lenq」及び「lenIDI」を用いて、(lenq−lenIDI−1)ビットの乱数「R1」を生成する。ここで、乱数「R1」の最上位ビットは1とする。

乱数生成部2403は、生成した乱数「R1」を素数候補生成部2404へ出力する。

また、乱数生成部2403は、第1素数判定部2405及び第2素数判定部2406の何れかから、再度乱数を生成する旨の第2生成指示を受け付けると、各ビットサイズを読み出し、上記の動作を行う。

[0392] ＜素数候補生成部2404＞

素数候補生成部2404は、生成された数を記憶する生成情報記憶領域とを有している。

素数候補生成部2404は、受付部2401より開始指示を受け取ると、第1生成指示を乱数生成部2403へ出力する。

[0393] 素数候補生成部2404は、乱数「R1」を乱数生成部2403より受け取ると、受付情報記憶部2402にて記憶している素数「q」及び発行識別子情報「IDI」を読み出す。

素数候補生成部2404は、読み出した素数「q」及び発行識別子情報「IDI」と、乱数生成部2403より受け取った乱数「R1」とを用いて、数「R＝IDI×R1」と、数「N＝2×R×q＋1」とを生成する。

[0394] 素数候補生成部2404は、生成した数「N」のビットサイズが「2×lenq」であるか否かを判断する。

「2×lenq」であると判断する場合には、素数候補生成部2404は、生成した数「N」を第1素数判定部2405へ出力し、生成した数「R」を生成情報記憶領域に記憶する。

[0395] 「2×lenq」でないと判断する場合には、素数候補生成部2404は、乱数生成部2403より受け取った乱数「R1」に2を掛けて、その結果を「R1」として、再度、上記の動作を行い、数「R」及び「N」を生成する。

素数候補生成部2404は、生成した数「N」のビットサイズが、「2×lenq」となるまで、上記の動作を繰り返す。

[0396] ＜第1素数判定部2405＞

第1素数判定部2405は、第1の実施の形態にて示す第1素数判定部143と同様の動作であるため、ここでの説明は省略する。

＜第2素数判定部2406＞

第2素数判定部2406は、第1の実施の形態にて示す第2素数判定部144と同様の動作であるため、ここでの説明は省略する。

[0397] なお、第2素数判定部2406は、判定により、生成した数「N」が素数であると判断する場合には、生成した数「N」を素数「N」として出力する。

＜素数生成装置2400の動作＞

以下に、素数生成装置2400の動作について説明する。

(素数生成処理)

ここでは、素数生成装置2400にて行われる素数生成処理について、図39に示す流れ図を用いて、変更点のみ説明する。

[0398] 素数生成装置2400は、ステップS2000において、素数「q」、素数「q」のビットサイズ「lenq」、発行識別子情報「IDI」及び発行識別子情報のビットサイズ「lenIDI」を受け付け、受け付けた各情報を受付情報記憶部2402へ書き込むように変更する。

素数生成装置2400は、上記のように変更されたステップS2000の実行後、ステップS2005を省略し、以下のように変更されたステップS2010を実行する。素数生成装置2400は、ステップS2010において、(lenq−lenIDI−1)ビットの乱数「R1」を生成するように変更する。

[0399] 以降の動作の流れは、図39と同様であるため、説明は省略する。

(素数候補生成処理)

ここでは、素数候補生成処理について、図40に示す流れ図を用いて、変更点のみ

説明する。

先ず、ステップS2050を、数「R＝IDI×R1」を生成するように変更する。

[0400] 次に、ステップS2055を、数「N＝2×R×q＋1」を生成するように変更する。

以降の動作の流れは、図40と同様であるため、説明は省略する。

(8)第1の実施の形態における素数生成部116を、予め記憶している8ビットの素数から256ビットの素数を生成する第1素数生成部と、256ビットの素数から512ビットの素数を生成する第2素数生成部とからなるとしてもよい。また、第1素数生成部及び第2素数生成部を、それぞれ個別の素数生成装置としてもよい。

[0401] 第1素数生成部は、従来と同様の方法にて、8ビットの素数から128ビットの素数を生成し、上記に示す素数生成装置2200を適用して、128ビットの素数から256ビットの素数を生成する。

以下に、第2素数生成部の構成の一例を、図44に示す。ここでは、第2素数生成部を1つの素数生成装置2500として説明する。素数生成装置2500は、素数「q」と、そのビットサイズ「lenq」(ここでは、ビットサイズを256ビットとする。)と、発行識別子情報「IDI」と、そのビットサイズ「lenIDI」と、検証値「c」が与えられた場合に、(2×lenq)ビットからなる素数「N」を出力する。

[0402] 素数生成装置2500は、図44に示すように、受付部2501、受付情報記憶部2502、乱数生成部2503、素数候補生成部2504、第1素数判定部2505及び第2素数判定部2506から構成されている。

素数生成装置2500は、具体的には、マイクロプロセッサ、ROM、RAM、ハードディスクユニット、ディスプレイユニット、キーボード、マウスなどから構成されるコンピュータシステムである。前記RAM又は前記ハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することにより、素数生成装置2500は、その機能を達成する。

[0403] ＜受付情報記憶部2502＞

受付情報記憶部2502は、素数「N」を生成する際に与えられた素数「q」、素数「q」のビットサイズ「lenq」、発行識別子情報「IDI」、発行識別子情報のビットサイズ「lenIDI」及び検証値「c」を記憶する領域を備えている。

＜受付部2501＞

受付部2501は、素数「q」、素数「q」のビットサイズ「lenq」、発行識別子情報「IDI」、発行識別子情報のビットサイズ「lenIDI」及び検証値「c」を、外部（例えば、上記に示す第1素数生成部）より受け付け、受付部2501は、受け付けた素数「q」、そのビットサイズ「lenq」、発行識別子情報「IDI」、そのビットサイズ「lenIDI」及び検証値「c」を受付情報記憶部2502へ書き込む。

[0404] 受付部2501は、処理を開始する旨の開始指示を素数候補生成部2504へ出力する。

＜乱数生成部2503＞

乱数生成部2503は、乱数を生成する旨の第1生成指示を、素数候補生成部2504から受け取ると、素数「q」のビットサイズ「lenq」と、発行識別子情報「IDI」のビットサイズ「lenIDI」とを受付情報記憶部2502より読み出す。

[0405] 乱数生成部2503は、読み出したビットサイズ「lenq」及び「lenIDI」を用いて、(lenq−lenIDI−1)ビットの乱数「R1」を生成する。ここで、乱数「R1」の最上位ビットは1とする。

乱数生成部2503は、生成した乱数「R1」を素数候補生成部2504へ出力する。

また、乱数生成部2503は、第1素数判定部2505及び第2素数判定部2506の何れかから、再度乱数を生成する旨の第2生成指示を受け付けると、各ビットサイズを読み出し、上記の動作を行う。

[0406] ＜素数候補生成部2504＞

素数候補生成部2504は、生成された数を記憶する生成情報記憶領域とを有している。

素数候補生成部2504は、受付部2501より開始指示を受け取ると、第1生成指示を乱数生成部2503へ出力する。

[0407] 素数候補生成部2504は、乱数「R1」を乱数生成部2503より受け取ると、受付情報記憶部2502にて記憶している素数「q」、発行識別子情報「IDI」及び検証値「c」を読み出す。

素数候補生成部2504は、読み出した素数「q」、発行識別子情報「IDI」及び検証

値「c」と、乱数生成部2503より受け取った乱数「R1」とを用いて、数「R＝IDI×R1」と、数「N＝2×(R＋w)×q＋1」とを生成する。

[0408] ここで、「w」は「2×w×q＋1＝c mod IDI、0≦w＜IDI」を満たす数である。「w」は、「w＝(c−1)×m mod IDI」を計算することにより求める。「m」は「(2×q)×m＝1 mod IDI」を満たす数である。

素数候補生成部2504は、生成した数「N」のビットサイズが「2×lenq」であるか否かを判断する。

[0409] 「2×lenq」であると判断する場合には、素数候補生成部2504は、生成した数「N」を第1素数判定部2505へ出力し、生成した数「R」を生成情報記憶領域に記憶する。

「2×lenq」でないと判断する場合には、素数候補生成部2504は、乱数生成部2503より受け取った乱数「R1」に2を掛けて、その結果を「R1」として、再度、上記の動作を行い、数「R」及び「N」を生成する。

[0410] 素数候補生成部2504は、生成した数「N」のビットサイズが、「2×lenq」となるまで、上記の動作を繰り返す。

＜第1素数判定部2505＞

第1素数判定部2505は、第1の実施の形態にて示す第1素数判定部143と同様の動作であるため、ここでの説明は省略する。

[0411] ＜第2素数判定部2506＞

第2素数判定部2506は、第1の実施の形態にて示す第2素数判定部144と同様の動作であるため、ここでの説明は省略する。

なお、第2素数判定部2506は、判定により、生成した数「N」が素数であると判断する場合には、生成した数「N」を素数「N」として出力する。

[0412] ＜素数生成装置2500の動作＞

以下に、素数生成装置2400の動作について説明する。

(素数生成処理)

ここでは、素数生成装置2500にて行われる素数生成処理について、図39に示す流れ図を用いて、変更点のみ説明する。

[0413] 素数生成装置2500は、ステップS2000において、素数「q」、素数「q」のビットサイズ「lenq」、発行識別子情報「IDI」、発行識別子情報のビットサイズ「lenIDI」及び検証値「c」を受け付け、受け付けた各情報を受付情報記憶部2502へ書き込むように変更する。

素数生成装置2500は、上記のように変更されたステップS2000の実行後、ステップS2005を省略し、以下のように変更されたステップS2010を実行する。素数生成装置2500は、ステップS2010において、(lenq−lenIDI−1)ビットの乱数「R1」を生成するように変更する。

[0414] 以降の動作の流れは、図39と同様であるため、説明は省略する。

(素数候補生成処理)

ここでは、素数候補生成処理について、図40に示す流れ図を用いて、変更点のみ説明する。

先ず、ステップS2050を、数「R＝IDI×R1」を生成するように変更する。

[0415] 次に、ステップS2055を、数「N＝2×(R＋w)×q＋1」を生成するように変更する。

以降の動作の流れは、図40と同様であるため、説明は省略する。

(9) 上記第1の実施の形態において、素数生成部116は、単射関数「f」を施し、その後、発行識別子情報「IDI」の埋め込みを行ったが、単射関数「f」を施すだけでもよいし、発行識別子情報「IDI」の埋め込みのみを行ってもよい。

[0416] 単射関数を施しただけの場合には、生成される素数は一意性が満たされる。このとき、単射関数を施すタイミングは、いつでもよい。

発行識別子情報「IDI」の埋め込みのみを行う場合には、生成された素数の一意性は満たされないが、生成された鍵の正当性の確認は、「IDI」を用いて行うことができる。なお、発行識別子情報「IDI」の埋め込みのみを行う場合は、256ビットの素数から512ビットの素数を生成するタイミングに行う。

[0417] また、第2の実施の形態においても同様である。

(10) 上記第1及び第2の実施の形態において、制御情報が「情報B」である場合に、素数生成部116は、単射関数を施し、数「R＝f(IDI｜｜R1)」を生成したが、これ

に限定されない。

例えば、制御情報が「情報B」である場合に、素数生成部116は、数「R＝f(R1｜｜IDI)」を生成してもよいし、数「R＝f(IDI)｜｜R1」を生成してもよし、数「R＝R1｜｜f(IDI)」を生成してもよい。

[0418] また、単射関数を用いないで、数「R＝(IDI｜｜R1)」を生成してもよいし、数「R＝R1｜｜IDI」を生成してもよい。

また、発行識別子情報「IDI」のビット列に、乱数「R1」を構成する各ビットを埋め込み、埋め込んだ結果(以下、「IDI__R1」という。)に単射関数「f」を施して数「R」を生成してもよい。

[0419] その一例を図45に示す。発行識別子情報「IDI」は、上述したように具体的には、64ビットからなり、そのビット列を「$S_1S_2S_3S_4\cdots S_{62}S_{63}S_{64}$」とする。乱数「R1」は、具体的には、63ビットからなり、そのビット列を「$T_1T_2T_3T_4\cdots T_{61}T_{62}T_{63}$」とする。ここで、「$S_n$」及び「$T_m$」は、「0」及び「1」の何れかである。なお、「n」は1以上64以下の数であり、「m」は1以上63以下の数である。このとき、数「IDI__R1」のビット列は、「$S_1T_1S_2T_2S_3T_3S_4T_4\cdots T_{61}S_{62}T_{62}S_{63}T_{63}S_{64}$」となる。

[0420] なお、一例では、発行識別子情報「IDI」のビット列に対して、1ビット置きに、乱数「R1」の各ビットを埋め込んだが、これに限定されない。発行識別子情報「IDI」のビット列に対して、複数ビット置きに、乱数「R1」の各ビットを埋め込んで、数「IDI__R1」を生成してもよい。このとき、「IDI」のビット列の間に埋め込まれないビット全てを、「IDI」のビット列における末尾のビット以降に、結合して、「IDI__R1」を生成する。

[0421] また、乱数「R1」のビット列に対して、発行識別子情報「IDI」の各ビットを埋め込んで、数「IDI__R1」を生成してもよい。例えば、1ビット置きに埋め込む場合には、数「IDI__R1」のビット列は、「$T_1S_1T_2S_2T_3S_3T_4S_4\cdots T_{62}S_{62}T_{63}S_{63}S_{64}$」となる。

また、発行識別子情報「IDI」と乱数「R1」とから、数「IDI__R1」を生成し、生成した数「IDI__R1」に単射関数「f」を施して数「R」を生成したが、これに限定されない。数「R」は、「R＝IDI__R1」としてもよい。

[0422] (11)上記第1の実施の形態において、制御情報が「情報A」である場合に、素数生成部116は、発行識別子情報「IDI」の埋め込みを行ったが、埋め込む情報は、「IDI

」に限定されない。

例えば、鍵発行サーバ100と証明書発行サーバ200とだけが既知の秘密関数であり、且つ1対1の関数である「g」を用いた値であってもよい。このとき、「IDI」の代わりに埋め込む値は、「g(IDI)」である。

[0423] また、第2の実施の形態においても同様である。

(12)上記第1の実施の形態において、鍵発行サーバ100と端末装置300との間に、安全な通信経路を確立して、鍵発行サーバ100から端末装置300へ、秘密鍵及び公開鍵の送付を行ったが、これに限定されない。

例えば、端末装置300の製造時に、鍵発行サーバ100と端末装置300とを、入出力装置を介して、秘密鍵及び公開鍵の送付を行ってもよい。

[0424] また、第2の実施の形態においても同様である。

(13)上記第1及び第2の実施の形態において、端末装置の具体例として、携帯電話機としたが、これに限定されない。

暗号化されたデータをネットワークを介して受信し、復号できる端末装置であればよい。

[0425] 例えば、パーソナルコンピュータや、PDA(Personal Digital Assistants)である。

(14)上記第1及び第2の実施の形態において、発行識別子情報「IDI」は、奇数であるとしたが、素数生成に検証値を用いない場合には、発行識別子情報「IDI」は、奇数でなくてもよい。

[0426] このとき、サーバ識別子と、カウンタにより、1から順に生成される発行識別子「PID」とを用いて生成する場合には、このとき、識別子生成部115は、素数を発行(生成)するたびに、数「1」をインクリメントしていくことで、容易に毎回異なる素数を生成できることになる。

(15)第1及び第2の実施の形態にて、生成する秘密鍵である素数のビットサイズは512ビットに限らない。1024ビットであっても、2048ビットであってもよい。このとき、素数生成部116は、秘密鍵である素数のビットサイズ(ここでは、「lenN」とする。)に対して、(lenN／4)ビットからなる素数を、従来の素数の生成方法により生成し、その

後、単射関数「f」を施して、(lenN／2)ビットからなる素数を生成し、最後に、発行識別子情報「IDI」を埋め込んだ「lenN」ビットからなる素数「N」を生成する。

[0427] なお、発行識別子情報「IDI」の埋め込みのみを行う場合には、素数生成部は、(lenN／2)ビットからなる素数を、従来の素数の生成方法により生成し、最後に、発行識別子情報「IDI」を埋め込んだ「lenN」ビットからなる素数「N」を生成する。

また、単射関数「f」を施し、一意な素数を生成するのみの場合は、(lenN／2)ビットからなる素数を、従来の素数の生成方法により生成し、その後、単射関数「f」を施して、「lenN」ビットからなる素数を生成する。

[0428] (16)第1の実施の形態における素数生成部116を、1つの素数生成装置としてもよい。このとき、この素数生成装置は、整数lenと発行識別子情報IDIを入力とし、lenビットの素数を出力するとしてもよい。

また、上述したように、第1実施の形態における素数生成部116は、素数情報生成部133の代わりに、素数生成の変形例1、2及び3にて示す素数情報生成部133A、素数情報生成部133B及び素数情報生成部133Cの何れかを用いてもよい。

[0429] また、第1実施の形態における素数生成部116は、8ビットの素数から512ビットの素数を生成する際に、発行識別子情報「IDI」を埋め込まないで、単射関数「f」を1回のみ施してもよい。このとき、証明書発行サーバ200では、証明書発行依頼情報と、公開鍵を受け取ると、正当性の確認を行わないで、公開鍵証明書「Cert」を発行する。

[0430] (17)素数に発行識別子情報を含ませる方法は、実施の形態に限らない。例えば、下位lenIDIビットがIDIである素数を生成・発行するとしてもよい。

(18)鍵発行サーバは3台に限定されない。鍵発行サーバは1台以上であればよい。このとき、各鍵発行サーバにて行う素数の生成方法は、同一の方法を用いる。

(19)第1の実施の形態における第2素数判定部144は、素数の判定に用いる条件式は、上記に示す(eq2)に限定されない。

[0431] 条件式「GCD(2^(2R)−1、N)＝1」を用いて、第2素数判定部144は、第1素数判定部143より受け取った数「N」が、当該条件式を満たすか否かを判断し、満たすと判断する場合に、数「N」を素数「N」としてもよい。

(20)第1の実施の形態において、鍵発行サーバ100は、端末装置300へ秘密鍵と公開鍵証明書を配布したが、これに限定されない。鍵発行サーバ100は、端末装置300へ秘密鍵のみを配布してもよい。このとき、鍵発行サーバ100は、公開鍵証明書を第三者に対して、公開する。または、鍵発行サーバ100は、公開鍵を第三者に対して、公開する。

[0432] (21)第1の実施の形態において、素数生成部116は、出力カウンタ136にて、鍵判定部117へ出力した素数の個数を管理したが、これに限定されない。

鍵判定部117にて、受け取った素数の個数をカウントしてもよい。この場合の一例を、以下に示す。

素数生成部116は、識別子生成部115から素数の生成開始命令を受け取ると、素数「p1」を生成し、生成した素数「p1」を鍵判定部117へ出力する。素数生成部116は、鍵判定部117から次の素数の要求を受け取ると、素数「p2」を生成し、生成した素数「p2」を鍵判定部117へ出力する。なお、素数「p1」及び「p2」の生成は、第1の実施の形態と同様であるため、説明は省略する。

[0433] 鍵判定部117は、カウンタ(初期値は「0」である。)を用いて、素数生成部116より素数を受け取ると、カウンタに「1」をインクリメントし、その結果が、1であるか否かを判断する。1であると判断する場合には、鍵判定部117は、素数生成部116へ、次の素数を要求する。1でないと判断する場合には、鍵判定部117は、素数「p1」と「p2」とが、一致するか否かの判断を行う。以降の動作は、第1の実施の形態と同様であるため、説明は省略する。

[0434] (22)上記第1及び第2の実施の形態において、発行識別子情報「IDI」のビットサイズを64ビットとしたが、これに限定されない。(lenq−1)よりも小さいビットサイズであればよい。

また、素数生成の変形例3において、素数「qg」のビットサイズを64ビットとしたが、これに限定されない。素数「qg」は、ビットサイズ「lenqg」が「(2×lenqg)＜(lenq−1)」を満たす素数であればよい。このとき、発行識別子情報は、そのビットサイズが、素数「qg」のビットサイズより小さければよい。

[0435] (23)証明書発行サーバ200の発行公開鍵確認部214において、公開鍵「PK＝(

n、e)」が、発行識別子情報「IDI」を用いて生成されたか否かを確認する方法について、「n−(c11×c12)」が、「IDI」で割り切れるか否かを検証するとしている。ここで、検証方法の具体例を示す。

検証方法の具体的な動作の流れを、図46に示す流れ図を用いて説明する。

[0436] 発行公開鍵確認部214は、数「n−(c11×c12)」を「Q」とする(ステップS2500)。

次に、発行公開鍵確認部214は、「Q−IDI」を算出し、算出結果を、再度、「Q」とする(ステップS2505)。

発行公開鍵確認部214は、数「Q」が、発行識別子情報「IDI」より小さいか否かを判断する(ステップS2510)。

[0437] 小さいと判断する場合には(ステップS2510における「YES」)、発行公開鍵確認部214は、数「Q」が「0」であるか否かを判断する(ステップS2515)。

「0」であると判断する場合には(ステップS2515における「YES」)、検証結果「0」を出力する(ステップS2520)。「0」でないと判断する場合には(ステップS2515における「NO」)、検証結果「1」を出力する(ステップS2525)。

[0438] 数「Q」が、発行識別子情報「IDI」以上であると判断する場合には(ステップS2510における「NO」)、ステップS2505へ戻る。

この動作により、公開鍵「PK=(n、e)」が、発行識別子情報「IDI」を用いて生成されたか否かを確認することができる。

発行公開鍵確認部214は、図18に示すステップS670にて、上記の検証処理を実行後、出力された検証結果が「0」である場合には、公開鍵「PK」は発行識別子情報「IDI」を用いて生成されたと判断し、検証結果が「1」である場合には、公開鍵「PK」は発行識別子情報「IDI」を用いて生成されていないと判断する。

[0439] (24)素数候補生成部142にて生成された数「N」が、「lenN=2×lenq」を満たさない場合、「R1=2×R1」としているが、その演算の具体例を以下に示す。

素数候補生成部142は、生成された数「N」が、「lenN=2×lenq」を満たさない場合には、数「R1」のビット列を、左に1ビット分だけシフトする。このとき、末尾のビットには「0」が設定される。これにより、「R1=2×R1」とすることできる。

[0440] (25)第1及び第2の実施の形態において、数「N」を算出する際に、「N=2×(R+

w)×q+1」としたが、これに限定されない。「N=2×R×q+c」としてもよい。

なぜなら、上記の実施の形態にて示した「w」及び「m」の条件式「w=(c−1)×m mod IDI」と、「(2×q)×m=1 mod IDI」とを用いると、「N=2×(R+w)×q+1」は、以下のように変形することができるからである。

[0441] $2\times(R+w)\times q+1=2\times R\times q+2\times w\times q+1$

$=2\times R\times q+2\times(c-1)\times m\times q+1$

$=2\times R\times q+2\times(c-1)\times(1/2q)\times q+1$

$=2\times R\times q+(c-1)+1$

$=2\times R\times q+c$

これにより、「N=2×(R+w)×q+1」の代わりに、「N=2×R×q+c」としてもよいことがわかる。

[0442] なお、「c」は検証値であり、出力カウンタの値が「1」の場合には、検証値「c」は、「c11」となり、出力カウンタの値が「2」以上の場合には、検証値「c」は、「c12」となる。例えば、第1の実施の形態における証明書発行サーバ200は、「N−c11×c12」が、「IDI」で割り切れるか否かを判断することにより、生成された公開鍵の正当性を確認することができる。

[0443] (26)第1の実施の鍵発行システム1において、鍵発行サーバにて生成された素数の正当性を検証する素数検証装置を加えてもよい。

この場合における素数検証装置及び鍵発行サーバ100の動作について、以下に説明する。

素数検証装置は、証明書発行サーバと同様に、検証値テーブルを予め記憶している。

[0444] 鍵発行サーバ100は、素数生成部116にて素数「p1」を生成すると、生成した素数「p1」、発行識別子情報「IDI」及びサーバ識別子を、素数検証装置へ出力する。

素数検証装置は、鍵発行サーバ100より、素数「p1」、発行識別子情報「IDI」及びサーバ識別子を受け取ると、受け取ったサーバ識別子に対応する第1検証値「c11」を読み出し、読み出した第1検証値「c11」を用いて、「p1−c11」を算出し、算出結果が、「IDI」で割り切れるか否かを判断する。割り切れると判断する場合には、素数検

証装置は、素数「p1」の利用を許可する情報を鍵発行サーバ100へ出力する。割り切れないと判断する場合には、素数「p1」の利用を禁止する情報を鍵発行サーバ100へ出力する。

[0445] 鍵発行サーバ100の素数生成部116は、素数検証装置から、素数「p1」の利用を禁止する情報を受け取ると、再度、素数「p1」を生成して、上記動作を繰り返す。

鍵発行サーバ100の素数生成部116は、素数検証装置から、素数「p1」の利用を許可する情報を受け取ると、生成した素数「p1」を鍵判定部117へ出力し、素数「p2」を生成する。素数生成部116は、生成した素数「p2」、発行識別子情報「IDI」及びサーバ識別子を、素数検証装置へ出力する。

[0446] 素数検証装置は、鍵発行サーバ100より、素数「p2」、発行識別子情報「IDI」及びサーバ識別子を受け取ると、受け取ったサーバ識別子に対応する第2検証値「c12」を読み出し、読み出した第1検証値「c12」を用いて、「p1−c12」を算出し、算出結果が、「IDI」で割り切れるか否かを判断する。割り切れると判断する場合には、素数検証装置は、素数「p2」の利用を許可する情報を鍵発行サーバ100へ出力する。割り切れないと判断する場合には、素数「p2」の利用を禁止する情報を鍵発行サーバ100へ出力する。

[0447] 鍵発行サーバ100の素数生成部116は、素数検証装置から、素数「p2」の利用を禁止する情報を受け取ると、再度、素数「p2」を生成して、上記動作を繰り返す。

鍵発行サーバ100の素数生成部116は、素数検証装置から、素数「p2」の利用を許可する情報を受け取ると、生成した素数「p2」と判定開始命令とを鍵判定部117へ出力する。

[0448] 鍵発行サーバ100における以降の動作は、第1の実施の形態と同様であるため、説明は省略する。

なお、素数生成部116は、鍵判定部117より再生成命令を受け取った場合には、再度素数「p2」を生成し、上記の動作を繰り返す。

(27)第1及び第2の実施の形態において、第1及び第2検証値は、鍵発行サーバ毎に割り当てたが、これに限定されない。

[0449] 端末装置毎に第1及び第2検証値を割り当て、端末識別子と、端末装置毎に割り当

てられた第1及び第2検証値とからなるテーブルを鍵発行サーバ及び証明書発行サーバにて管理してもよい。

鍵発行サーバは、鍵発行の要求のあった端末装置に対応する第1及び第2検証値を用いて、素数「p1」及び「p2」を生成し、生成した「p1」及び「p2」を用いて、公開鍵及び秘密鍵を生成する。鍵発行サーバは、公開鍵証明書を要求する際には、公開鍵、発行識別子情報、サーバ識別子及び端末識別子を、証明書発行サーバへ送信する。

[0450] 証明書発行サーバは、受け取った端末識別子に対応する第1及び第2検証値を読み出し、読み出した検証値と、受け取った公開鍵、及び発行識別子情報とを用いて、公開鍵の正当性を検証する。

端末装置毎に、2つの検証値を割り当てることにより、公開鍵の一意性を保ちながら、端末装置毎に割り当てた公開鍵の正当性を検証することができる。

[0451] また、上記に示す素数検証装置を用いて、生成した素数毎に、正当な素数であるか否かの検証を行ってもよい。なお、素数検証装置は、端末識別子と、端末装置毎に割り当てられた第1及び第2検証値とからなるテーブルを有しているとする。

(28)第1及び第2の実施の形態において、端末装置と鍵発行サーバとを、それぞれ個別の装置としたが、端末装置にて鍵発行を行ってもよい。

[0452] このとき、端末装置は、例えば、第1の形態にて示す構成に加えて、鍵発行サーバ100の構成にて説明した識別子格納部、識別子生成部、素数生成部、鍵判定部、鍵生成部及び公開鍵格納部とを有する。

端末装置は、識別子生成部を用いて、端末識別子と、数「1」とから発行識別子情報「IDI＝TID｜｜1」を生成し、生成した発行識別子情報を識別子格納部にて記憶する。

[0453] 端末装置は、素数生成部、鍵判定部及び鍵生成部を用いて、公開鍵と秘密鍵とを生成し、生成した公開鍵を公開鍵格納部へ格納し、生成した秘密鍵を秘密鍵格納部へ格納する。

さらに、端末装置は、発行識別子情報と、公開鍵と、端末識別子と、証明書発行依頼情報とを、証明書発行サーバへ送信し、公開鍵証明書を、証明書発行サーバから

受信する。

また、端末装置は、ICカードであってもよい。この場合、ICカードは、鍵の生成及び格納を行う。なお、発行識別子情報の生成及び格納をもICカードが行ってもよい。このとき、ICカードと、証明書発行サーバとの通信は、証明書発行サーバとネットワーク接続された装置に、ICカードを装着することにより行う。

[0454] (29)端末識別子は、一例として、シリアル番号としているが、これに限定されない。

端末識別子は、ユーザの生体科学的特徴を示すバイオメトリックス情報であってもよい。バイオメトリックス情報は、例えば、ユーザの指紋の特徴を示す指紋情報、ユーザの声紋の特徴を示す声紋情報、ユーザの虹彩の特徴を示す虹彩情報、ユーザの顔の輪郭の特徴を示す輪郭情報、ユーザのDNAの特徴を示すDNA情報又は、これら情報の組合せである。

[0455] また、端末識別子の一部が、バイオメトリックス情報であるとしてもよい。

また、端末識別子は、端末装置を管理する管理サーバにて発行され、管理サーバからネットワークによる通信によって、与えられるものとしてもよい。または、管理サーバにて発行された端末識別子を、SDカード等の記録媒体によって、与えられるとしてもよい。

(30)本発明は、上記に示す方法であるとしてもよい。また、これらの方法をコンピュータにより実現するコンピュータプログラムであるとしてもよいし、前記コンピュータプログラムからなるデジタル信号であるとしてもよい。

[0456] また、本発明は、前記コンピュータプログラム又は前記デジタル信号をコンピュータ読み取り可能な記録媒体、例えば、フレキシブルディスク、ハードディスク、CD—ROM、MO、DVD、DVD—ROM、DVD—RAM、BD(Blu—ray Disc)、半導体メモリなど、に記録したものとしてもよい。また、これらの記録媒体に記録されている前記コンピュータプログラム又は前記デジタル信号であるとしてもよい。

[0457] また、本発明は、前記コンピュータプログラム又は前記デジタル信号を、電気通信回線、無線又は有線通信回線、インターネットを代表とするネットワーク等を経由して伝送するものとしてもよい。

また、本発明は、マイクロプロセッサとメモリとを備えたコンピュータシステムであって

、前記メモリは、上記コンピュータプログラムを記憶しており、前記マイクロプロセッサは、前記コンピュータプログラムに従って動作するとしてもよい。

[0458] また、前記プログラム又は前記デジタル信号を前記記録媒体に記録して移送することにより、又は前記プログラム又は前記デジタル信号を前記ネットワーク等を経由して移送することにより、独立した他のコンピュータシステムにより実施するとしてもよい。

(31)上記実施の形態及び上記変形例をそれぞれ組み合わせるとしてもよい。

産業上の利用可能性

[0459] 発明を構成する各サーバ及び各端末装置は、電器機器製造産業において、経営的に、また継続的及び反復的に、製造し、販売することができる。また、本発明を構成する各サーバ及び各端末装置は、インターネットを用いたサービス産業において、経営的に、また継続的及び反復的に使用することができる。

請求の範囲

[1] 既知の素数qより大きい素数候補Nを算出して素数判定する素数算出装置であって、

既知の素数qを記憶している素数記憶手段と、

素数の利用範囲における一意の管理情報を記憶している管理情報記憶手段と、

前記管理情報記憶手段から前記管理情報を読み出し、読み出した前記管理情報に依存する攪乱情報Rを生成する攪乱情報生成手段と、

前記素数記憶手段から前記素数qを読み出し、読み出した前記素数q及び生成された前記攪乱情報Rを用いて、N＝2×攪乱情報R×素数q＋1により、素数候補Nを算出する候補算出手段と、

算出された素数候補Nが素数であるか否かを判定する素数判定手段と、

素数であると判定される場合に、算出された素数候補Nを素数として出力する出力手段と

を備えることを特徴とする素数算出装置。

[2] 前記攪乱情報生成手段は、

前記管理情報記憶手段から前記管理情報を読み出す読出部と、

乱数rを算出する乱数算出部と、

読み出した前記管理情報と生成した乱数rとを結合する結合部と、

前記管理情報と乱数rとの結合体に基づいて、攪乱情報Rを算出する演算部と

を含むことを特徴とする請求項1に記載の素数算出装置。

[3] 前記演算部は、前記結合体に、単射の関数を施して攪乱情報Rを生成する

ことを特徴とする請求項2に記載の素数算出装置。

[4] 前記単射の関数は、排他的論理和であり、

前記演算部は、所定の鍵情報を予め記憶しており、前記鍵情報と前記結合体とに排他的論理和を施して攪乱情報Rを生成する

ことを特徴とする請求項3に記載の素数算出装置。

[5] 前記素数算出装置は、素数qの2倍のビット長を有する素数候補Nを算出し、

前記乱数算出部は、素数qのビット長から前記管理情報のビット長及び1を差し引

いて得られるビット長の前記乱数rを算出する

ことを特徴とする請求項3に記載の素数算出装置。

[6] 前記素数判定手段は、

前記素数候補Nに対して、$2^{N-1}=1 \mod N$を満たすか否かを判定する第1判定部と、

前記第1判定部により満たすと判定される場合に、さらに、素数候補N及び攪乱情報Rに対して、$2^{2R} \neq 1 \mod N$を満たすか否かを判定し、満たすと判定する場合に、素数候補Nが素数であると決定する第2判定部と

を含むことを特徴とする請求項5に記載の素数算出装置。

[7] 前記素数判定手段は、

前記素数候補Nに対して、$2^{N-1}=1 \mod N$を満たすか否かを判定する第1判定部と、

前記第1判定部により満たすと判定される場合に、さらに、素数候補N及び攪乱情報Rに対して、$GCD(2^{2R}-1, N)=1$を満たすか否かを判定し、満たすと判定する場合に、素数候補Nが素数であると決定する第2判定部と

を含むことを特徴とする請求項5に記載の素数算出装置。

[8] 前記素数算出装置は、さらに、

前記素数判定手段により素数であると判定されるまで、前記攪乱情報生成手段、前記候補算出手段及び前記素数判定手段に対して、攪乱情報Rの生成と、素数候補Nの算出と、前記判定とを繰り返すように制御する繰返制御手段

を含むことを特徴とする請求項1に記載の素数算出装置。

[9] 前記素数算出装置は、さらに、

乱数R'を算出する次段乱数算出手段と、

出力された前記素数N及び生成された前記乱数R'を用いて、N'＝2×乱数R'×素数N＋1により、素数候補N'を算出する次段候補算出手段と、

算出された素数候補N'が素数であるか否かを判定する次段素数判定手段と、

素数であると判定される場合に、算出された素数候補N'を素数として出力する次段出力手段と、

前記次段素数判定手段により素数であると判定されるまで、前記次段乱数算出手段、前記次段候補算出手段及び前記次段素数判定手段に対して、乱数R'の生成と、素数候補N'の算出と、前記判定とを繰り返すように制御する次段繰返制御手段とを含むことを特徴とする請求項8に記載の素数算出装置。

[10] 記素数算出装置は、さらに、

所定の検証値を記憶している次段情報記憶手段と、

乱数r'を生成する次段乱数生成手段と、

前記管理情報に生成した前記乱数r'を乗じて攪乱情報R'を算出し、N'＝2×攪乱情報R'×素数N＋検証値により、素数候補N'を算出する次段候補算出手段とを含み、

前記素数判定手段は、さらに、算出された素数候補N'が素数であるか否かを判定し、

前記出力手段は、さらに、素数候補N'が素数であると判定される場合に、算出された素数候補N'を素数として出力する

ことを特徴とする請求項8に記載の素数算出装置。

[11] 前記素数算出装置は、RSA暗号の公開鍵及び秘密鍵を生成する鍵生成装置であり、

前記素数算出装置は、さらに、

算出された素数Nを用いて、RSA暗号の公開鍵を生成する公開鍵生成手段と、

生成された公開鍵を用いて、RSA暗号の秘密鍵を生成する秘密鍵生成手段とを含む

ことを特徴とする請求項8に記載の素数算出装置。

[12] 前記公開鍵生成手段は、前記繰返制御手段に対して、新たに素数N'が得られるように指示し、前記素数N及び新たに得られた素数N'を用いて、n＝素数N×素数N'により、数nを算出し、乱数eを生成し、

算出された数nと生成された乱数eとの組が前記公開鍵であり、

前記秘密鍵生成手段は、e×d＝1 mod Lを満たすdを算出し、

Lは、素数N−1と素数N'−1との最小公倍数であり、

算出されたdが前記秘密鍵である

ことを特徴とする請求項11に記載の素数算出装置。

[13] 前記素数算出装置は、端末装置に対して、RSAの秘密鍵及び公開鍵を生成し、発行する鍵発行サーバ装置であり、

前記素数算出装置は、さらに、

生成した前記秘密鍵を、端末装置に対して出力する鍵出力手段と、

生成した前記公開鍵を、公開する公開手段とを含む

ことを特徴とする請求項11に記載の素数算出装置。

[14] 前記素数算出装置は、さらに、

前記端末装置を一意に識別する端末装置識別子を取得する識別子取得手段と、

取得した端末装置識別子を含む前記管理情報を生成する管理情報生成手段と、

生成した前記管理情報を前記管理情報記憶手段に書き込む書込手段とを

含むことを特徴とする請求項13に記載の素数算出装置。

[15] 前記素数算出装置は、さらに、

鍵発行サーバ装置としての当該素数算出装置を一意に識別するサーバ識別子を予め記憶しているサーバ識別子記憶手段を含み、

前記管理情報生成手段は、さらに、前記サーバ識別子記憶手段から前記サーバ識別子を読み出し、読み出したサーバ識別子をさらに含む前記管理情報を生成することを特徴とする請求項14に記載の素数算出装置。

[16] 既知の素数より大きい素数を算出する素数算出装置であって、

既知の入力素数の2倍のビット長を有する出力素数を算出する素数算出手段と、

既知の素数初期値を記憶している素数記憶手段と、

前記素数算出手段に対して、算出を複数回繰り返すように制御する繰返制御手段とを備え、

前記繰返制御手段は、前記繰返しにおける初回の算出において、前記素数記憶手段に記憶されている素数初期値を、前記入力素数として、前記素数算出手段に与え、

前記繰返しの初回の算出以外の他の算出において、1つ前の回の算出においてさ

れた出力素数を、当該他の算出における前記入力素数として、前記素数算出手段に与え、

前記複数回の算出のいずれか1の算出において、前記素数算出手段は、

素数の利用範囲における一意の管理情報を記憶している管理情報記憶部と、

前記管理情報記憶部から前記管理情報を読み出し、読み出した前記管理情報に依存する攪乱情報Rを生成する攪乱情報生成部と、

前記入力素数qを受け取り、受け取った前記入力素数q及び生成された前記攪乱情報Rを用いて、N＝2×攪乱情報R×素数q＋1により、素数候補Nを算出する候補算出部と、

算出された素数候補Nが素数であるか否かを判定する素数判定部と、

素数であると判定される場合に、算出された素数候補Nを出力素数として出力する出力部と、

前記素数判定部により素数であると判定されるまで、前記攪乱情報生成部、前記候補算出部及び前記素数判定部に対して、攪乱情報Rの生成と、素数候補Nの算出と、前記判定とを繰り返すように制御する繰返制御部とを含む

ことを特徴とする素数算出装置。

[17] 前記複数回の算出のうち、最終回の算出において、前記素数算出手段は、

所定の検証値を記憶している情報記憶部と、

乱数r'を生成する乱数生成部と、

前記管理情報に生成した前記乱数r'を乗じて攪乱情報R'を算出し、N'＝2×攪乱情報R'×1つ前の回において算出された出力素数＋検証値により、素数候補N'を算出する候補算出部と、

算出された素数候補N'が素数であるか否かを判定する素数判定部と、

素数候補N'が素数であると判定される場合に、算出された素数候補N'を素数として出力する出力部と、

前記素数判定部により素数であると判定されるまで、前記乱数生成部、前記候補算出部及び前記素数判定部に対して、乱数r'の生成と、素数候補N'の算出と、前記判定とを繰り返すように制御する繰返制御部とを含む

ことを特徴とする請求項16に記載の素数算出装置。

[18] 端末装置に対してRSAの秘密鍵及び公開鍵を生成して発行する鍵発行サーバ装置と、前記端末装置とから構成される鍵発行システムであって、

鍵発行サーバ装置は、

既知の素数qより大きい素数Nを算出する素数算出手段と、

算出された素数Nを用いて、RSA暗号の公開鍵を生成する公開鍵生成手段と、

生成された公開鍵を用いて、RSA暗号の秘密鍵を生成する秘密鍵生成手段と、

生成された前記秘密鍵を、端末装置に対して出力する鍵出力手段と、

生成された前記公開鍵を公開する公開手段とを備え、

前記素数算出手段は、

既知の素数qを記憶している素数記憶部と、

一意の管理情報を記憶している管理情報記憶部と、

前記管理情報記憶部から前記管理情報を読み出し、読み出した前記管理情報に依存する攪乱情報Rを生成する攪乱情報生成部と、

前記素数記憶部から前記素数qを読み出し、読み出した前記素数q及び生成された前記攪乱情報Rを用いて、N＝2×攪乱情報R×素数q＋1により、素数候補Nを算出する候補算出部と、

算出された素数候補Nが素数であるか否かを判定する素数判定部と、

素数であると判定される場合に、算出された素数候補Nを素数として出力する出力部と、

前記素数判定部により素数であると判定されるまで、前記攪乱情報生成部、前記候補算出部及び前記素数判定部に対して、攪乱情報Rの生成と、素数候補Nの算出と、前記判定とを繰り返すように制御する繰返制御部とを含み、

前記端末装置は、

前記秘密鍵を受け取る受信手段と、

受信した秘密鍵を記憶する鍵記憶手段と

を備えることを特徴とする鍵発行システム。

[19] 前記鍵発行システムは、さらに、証明書発行サーバ装置を含み、

前記鍵出力手段は、前記公開鍵を前記証明書発行サーバ装置へ出力し、

前記証明書発行サーバ装置は、

当該証明書発行サーバ装置の秘密鍵を記憶している記憶手段と、

前記公開鍵を取得する取得手段と、

前記証明書発行サーバ装置の秘密鍵を用いて、前記公開鍵を含む公開鍵情報に、デジタル署名を施して、署名データを生成し、少なくとも前記公開鍵及び生成した前記署名データを含む公開鍵証明書を生成する証明書生成手段と、

生成した公開鍵証明書を鍵発行サーバ装置へ出力する出力手段とを備える

ことを特徴とする請求項18に記載の鍵発行システム。

[20] 既知の素数qより大きい素数候補Nを算出して素数判定する素数算出装置で用いられる素数算出方法であって、

前記素数算出装置は、既知の素数qを記憶している素数記憶手段と、素数の利用範囲における一意の管理情報を記憶している管理情報記憶手段とを備え、

前記素数算出方法は、

前記管理情報記憶手段から前記管理情報を読み出し、読み出した前記管理情報に依存する攪乱情報Rを生成する乱数生成ステップと、

前記素数記憶手段から前記素数qを読み出し、読み出した前記素数q及び生成された前記攪乱情報Rを用いて、N＝2×攪乱情報R×素数q＋1により、素数候補Nを算出する候補算出ステップと、

算出された素数候補Nが素数であるか否かを判定する素数判定ステップと、

素数であると判定される場合に、算出された素数候補Nを素数として出力する出力ステップと

を含むことを特徴とする素数算出方法。

[21] 既知の素数qより大きい素数候補Nを算出して素数判定する素数算出装置で用いられる素数算出用のコンピュータプログラムであって、

前記素数算出装置は、既知の素数qを記憶している素数記憶手段と、素数の利用範囲における一意の管理情報を記憶している管理情報記憶手段とを備え、

前記素数算出用のコンピュータプログラムは、

前記管理情報記憶手段から前記管理情報を読み出し、読み出した前記管理情報に依存する攪乱情報Rを生成する乱数生成ステップと、

前記素数記憶手段から前記素数qを読み出し、読み出した前記素数q及び生成された前記攪乱情報Rを用いて、N＝2×攪乱情報R×素数q＋1により、素数候補Nを算出する候補算出ステップと、

算出された素数候補Nが素数であるか否かを判定する素数判定ステップと、

素数であると判定される場合に、算出された素数候補Nを素数として出力する出力ステップと

を含むことを特徴とするコンピュータプログラム。

[22] 前記コンピュータプログラムは、

コンピュータ読み取り可能な記録媒体に記録されている

ことを特徴とする請求項21に記載のコンピュータプログラム。

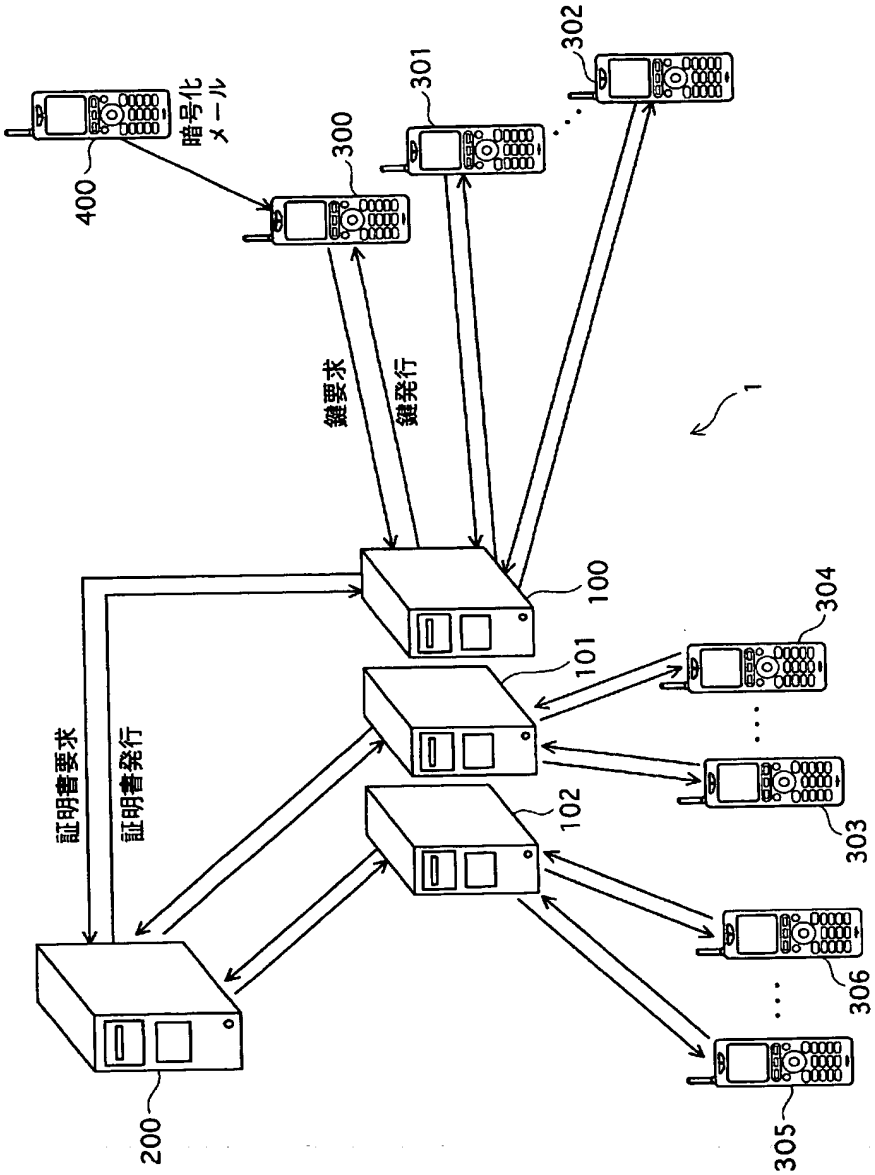
[23] 前記コンピュータプログラムは、

搬送波に乗せられて送信される

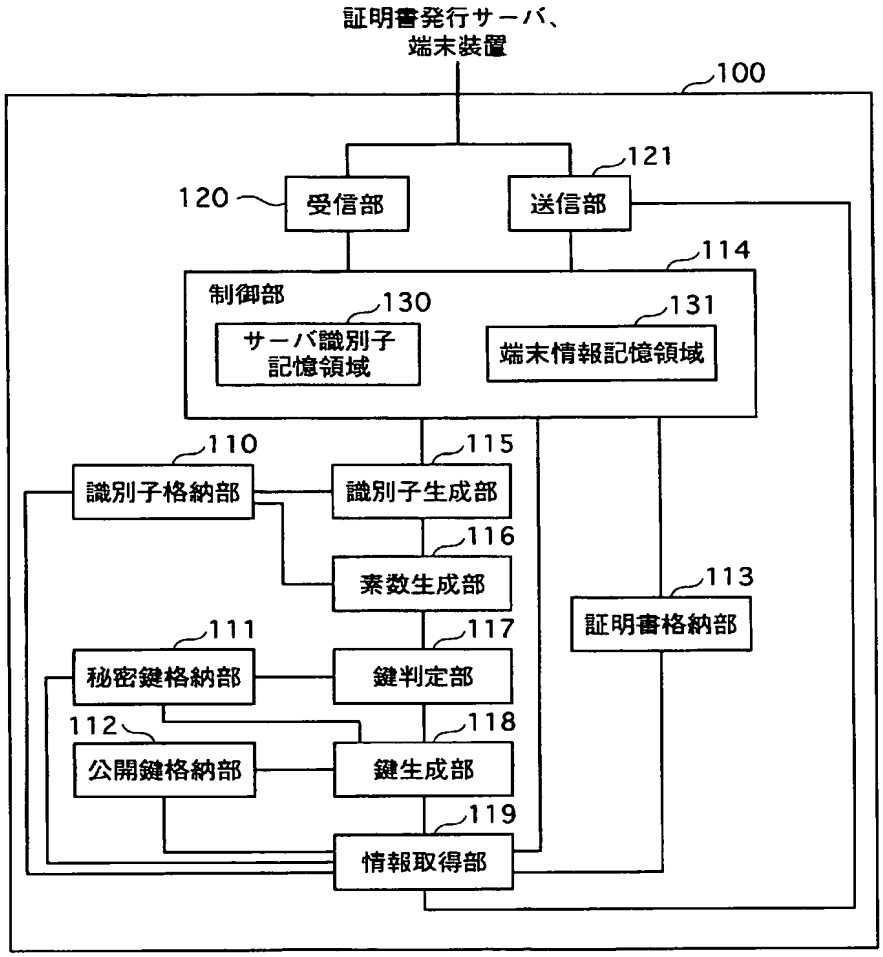
ことを特徴とする請求項21に記載のコンピュータプログラム。

WO 2005/064843 PCT/JP2004/019108

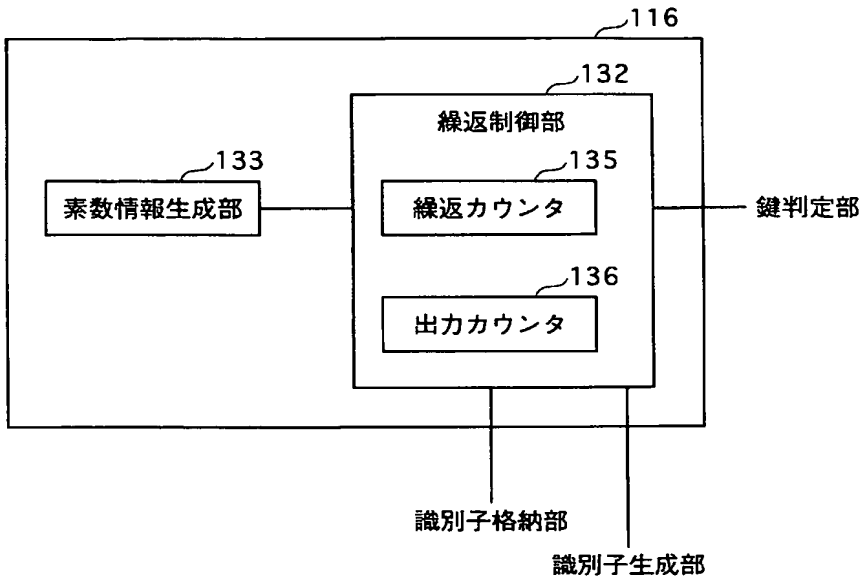
[図1]



[図2]


証明書発行サーバ、
端末装置
100
120
受信部
121
送信部
114
制御部
130
サーバ識別子
記憶領域
131
端末情報記憶領域
110
識別子格納部
115
識別子生成部
116
素数生成部
113
証明書格納部
111
秘密鍵格納部
117
鍵判定部
112
公開鍵格納部
118
鍵生成部
119
情報取得部

[図3]

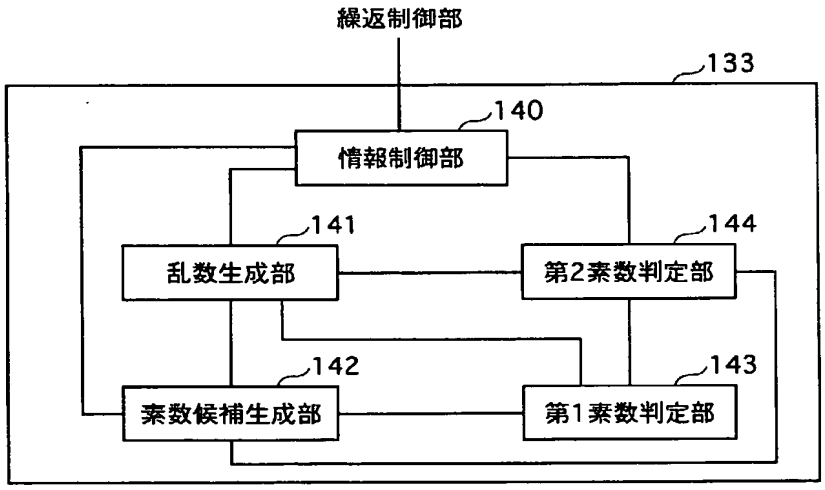

116
132
繰返制御部
133
素数情報生成部
135
繰返カウンタ
136
出力カウンタ
鍵判定部
識別子格納部
識別子生成部

[図4]

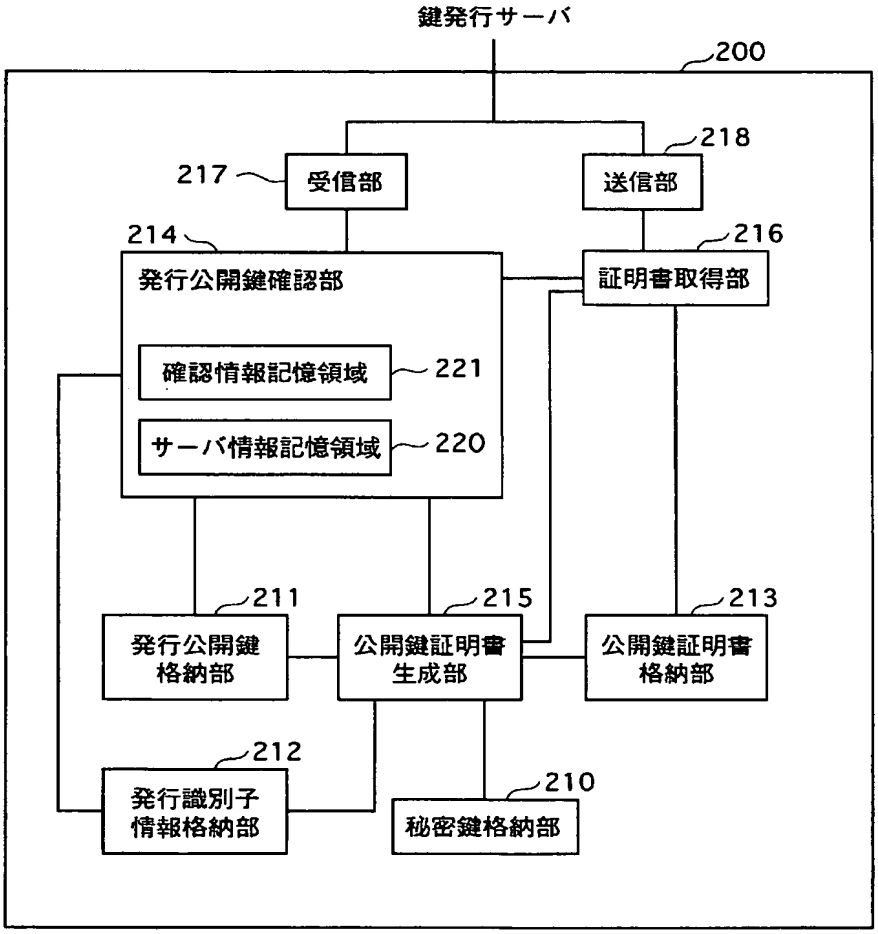
T100

回数	制御情報
1	情報C
2	情報C
3	情報C
4	情報C
5	情報B
6	情報A

[図5]


繰返制御部
133
140
情報制御部
141
乱数生成部
144
第2素数判定部
142
素数候補生成部
143
第1素数判定部

[図6]

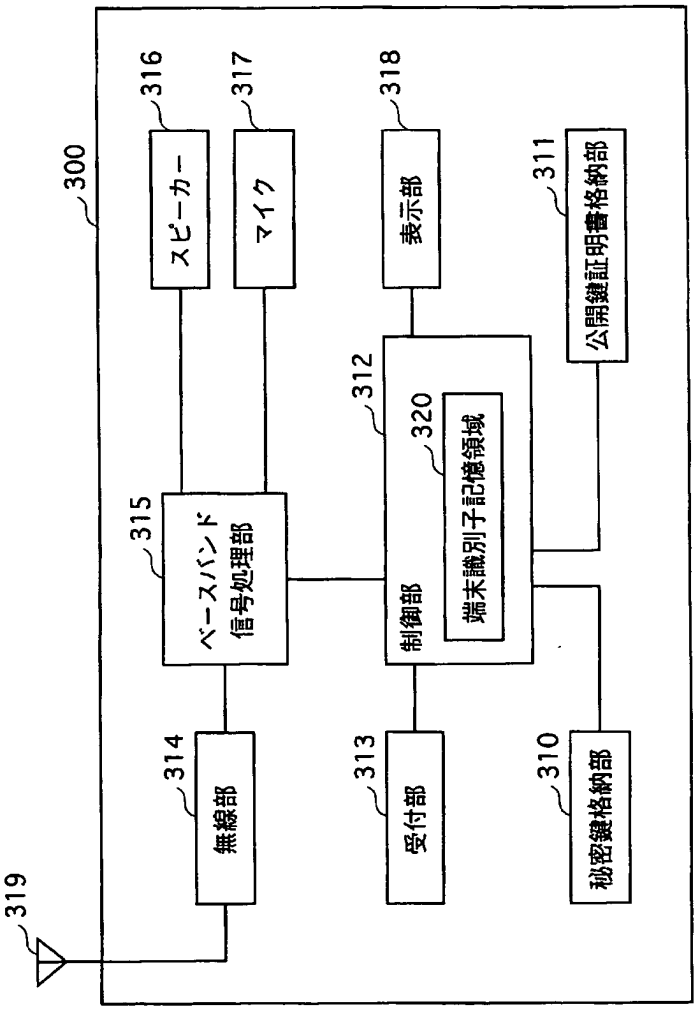

鍵発行サーバ
200
217
受信部
218
送信部
214
発行公開鍵確認部
216
証明書取得部
確認情報記憶領域
221
サーバ情報記憶領域
220
211
発行公開鍵格納部
215
公開鍵証明書生成部
213
公開鍵証明書格納部
212
発行識別子情報格納部
210
秘密鍵格納部

[図7]

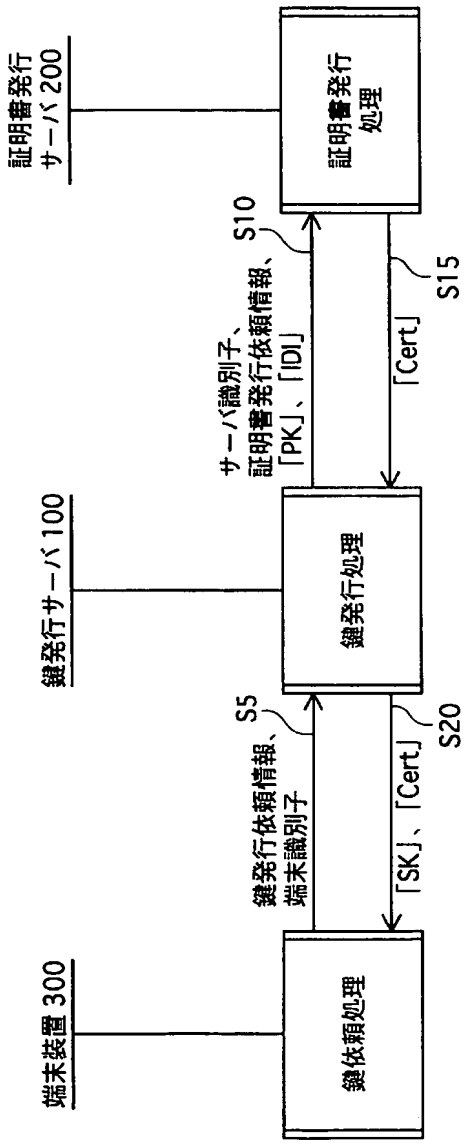
T200

サーバ識別子	第1検証値	第2検証値
SID A	c11	c12
SID B	c21	c22
SID C	c31	c33

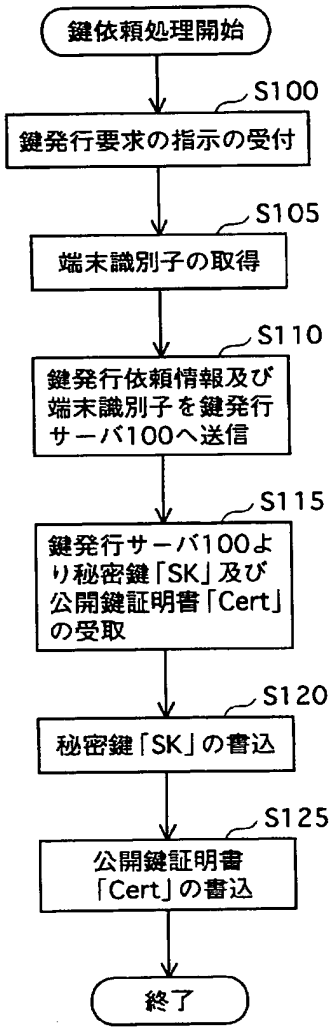
[図8]


300
316
スピーカー
317
マイク
318
表示部
311
公開鍵証明書格納部
315
ベースバンド
信号処理部
312
制御部
320
端末識別子記憶領域
314
無線部
313
受付部
310
秘密鍵格納部
319

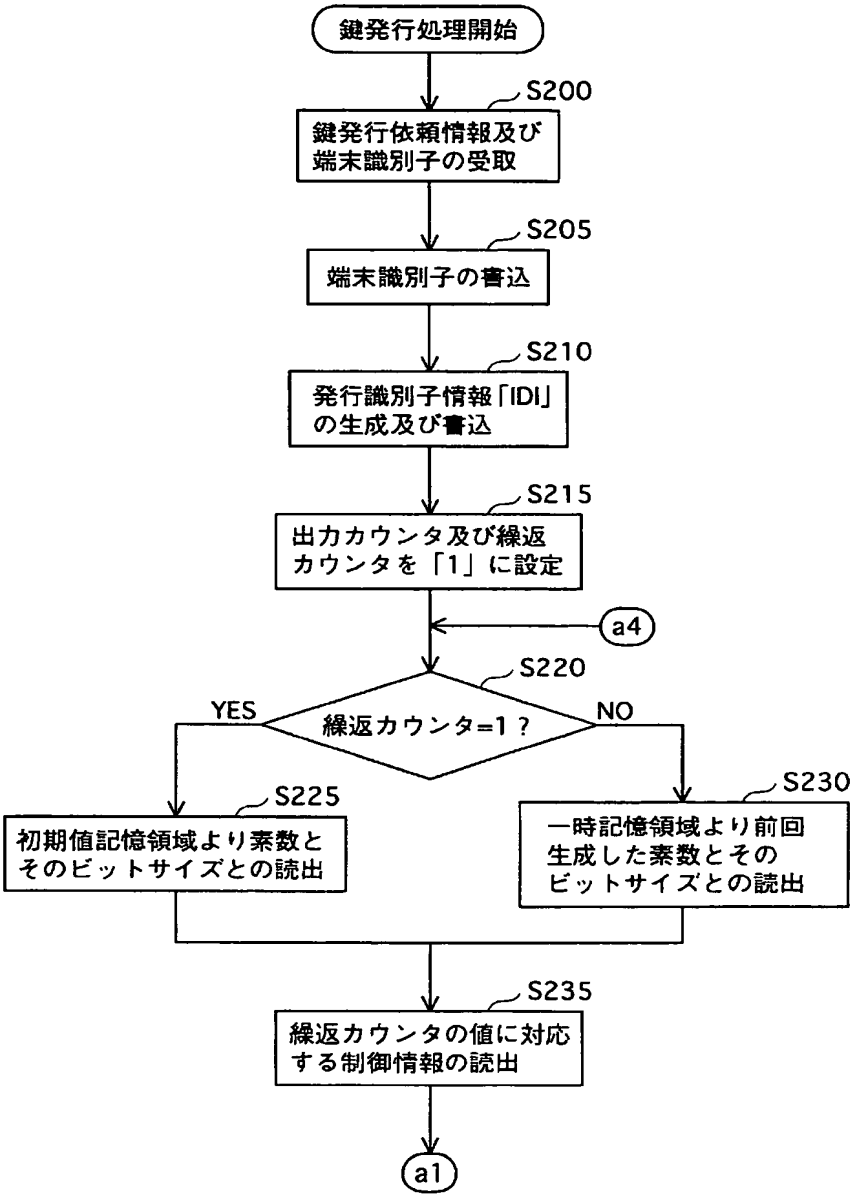
[図9]


証明書発行
サーバ200
証明書発行
処理
S10
サーバ識別子、
証明書発行依頼情報、
「PK」、「IDI」
S15
「Cert」
鍵発行サーバ100
鍵発行処理
S5
鍵発行依頼情報、
端末識別子
S20
「SK」、「Cert」
端末装置300
鍵依頼処理

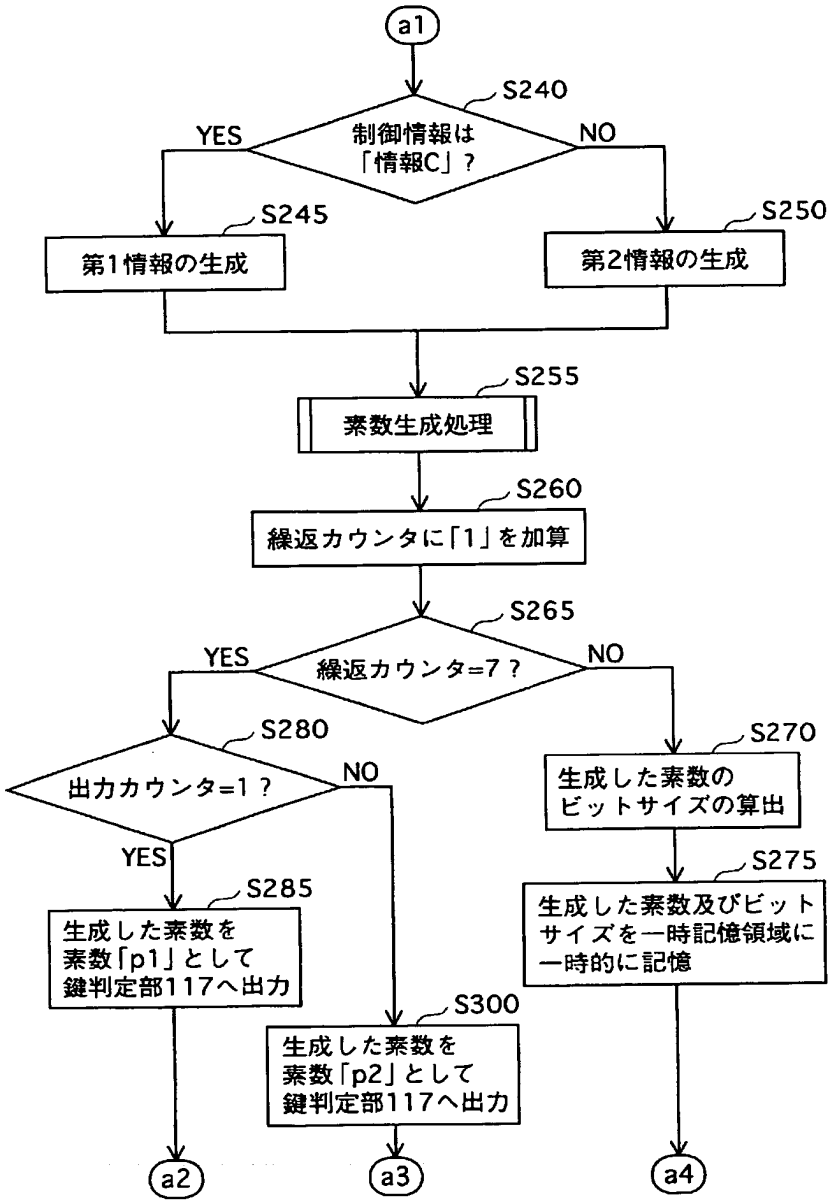
[図10]


鍵依頼処理開始
S100
鍵発行要求の指示の受付
S105
端末識別子の取得
S110
鍵発行依頼情報及び端末識別子を鍵発行サーバ100へ送信
S115
鍵発行サーバ100より秘密鍵「SK」及び公開鍵証明書「Cert」の受取
S120
秘密鍵「SK」の書込
S125
公開鍵証明書「Cert」の書込
終了

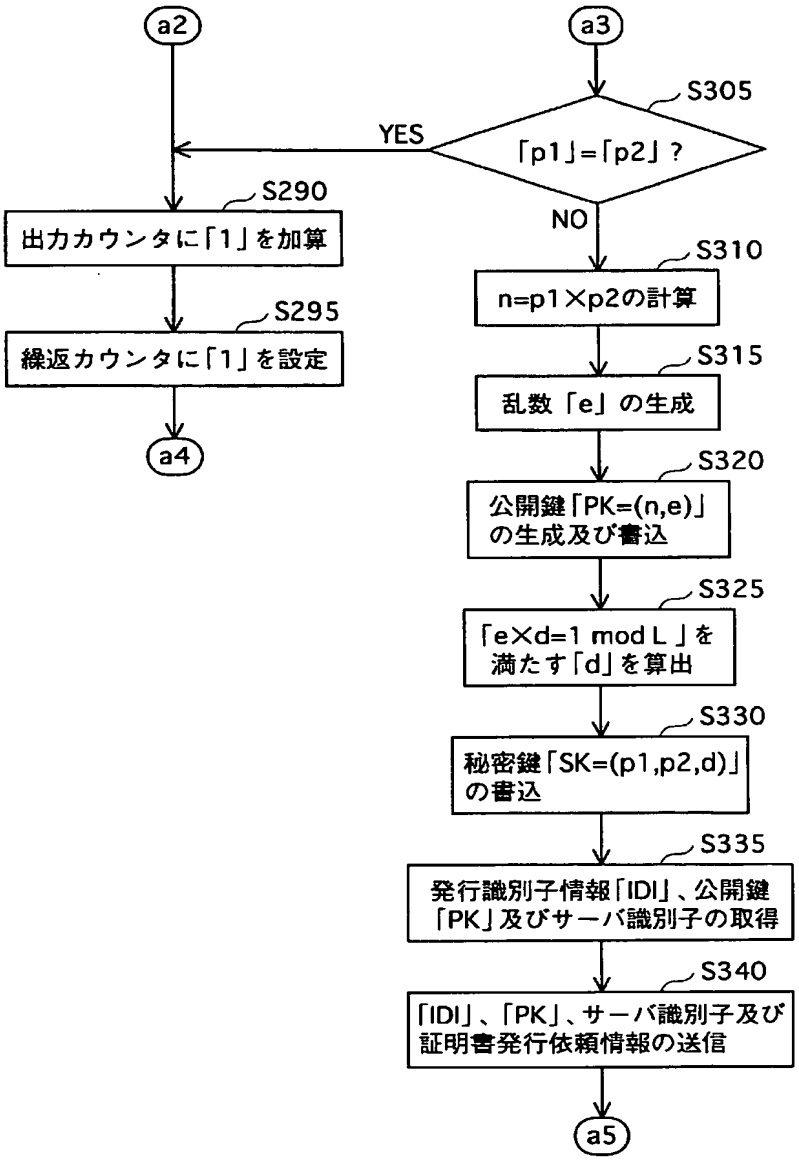
[図11]


鍵発行処理開始
S200
鍵発行依頼情報及び端末識別子の受取
S205
端末識別子の書込
S210
発行識別子情報「IDI」の生成及び書込
S215
出力カウンタ及び繰返カウンタを「1」に設定
a4
S220
繰返カウンタ=1？
YES
NO
S225
初期値記憶領域より素数とそのビットサイズとの読出
S230
一時記憶領域より前回生成した素数とそのビットサイズとの読出
S235
繰返カウンタの値に対応する制御情報の読出
a1

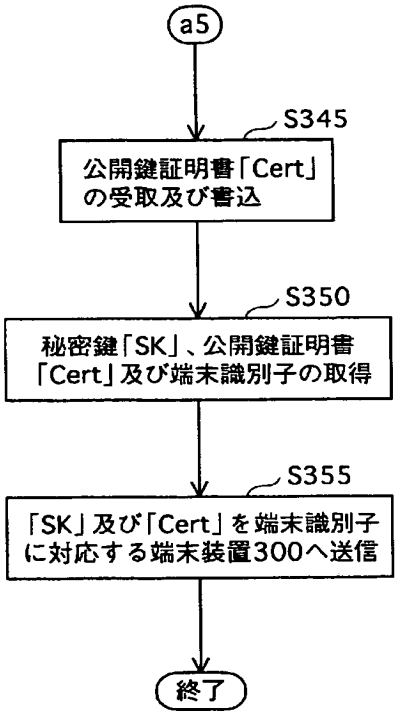
[図12]


a1
S240
制御情報は「情報C」？
YES
NO
S245
第1情報の生成
S250
第2情報の生成
S255
素数生成処理
S260
繰返カウンタに「1」を加算
S265
繰返カウンタ=7？
YES
NO
S280
出力カウンタ=1？
NO
YES
S285
生成した素数を素数「p1」として鍵判定部117へ出力
S270
生成した素数のビットサイズの算出
S275
生成した素数及びビットサイズを一時記憶領域に一時的に記憶
S300
生成した素数を素数「p2」として鍵判定部117へ出力
a2
a3
a4

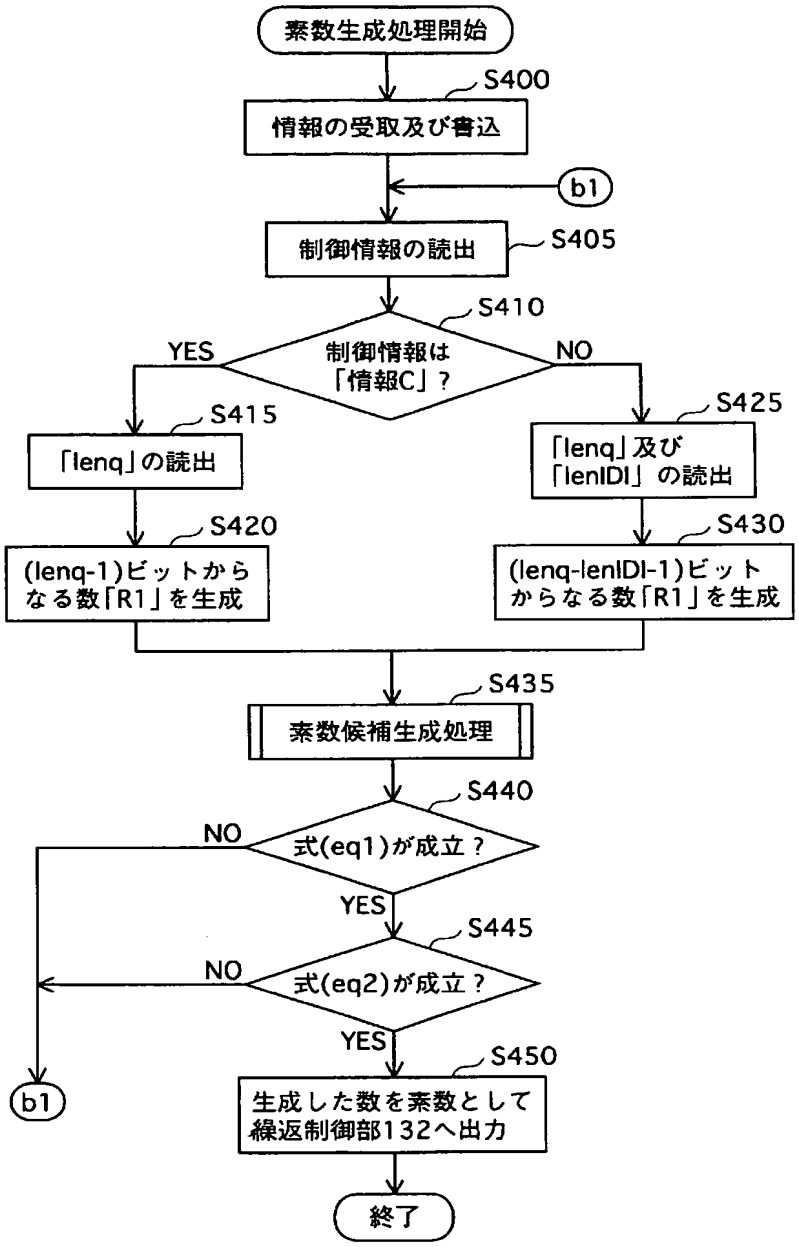
[図13]


a2
a3
S305
「p1」=「p2」?
YES
NO
S290
出力カウンタに「1」を加算
S295
繰返カウンタに「1」を設定
a4
S310
n=p1×p2の計算
S315
乱数「e」の生成
S320
公開鍵「PK=(n,e)」の生成及び書込
S325
「e×d=1 mod L」を満たす「d」を算出
S330
秘密鍵「SK=(p1,p2,d)」の書込
S335
発行識別子情報「IDI」、公開鍵「PK」及びサーバ識別子の取得
S340
「IDI」、「PK」、サーバ識別子及び証明書発行依頼情報の送信
a5

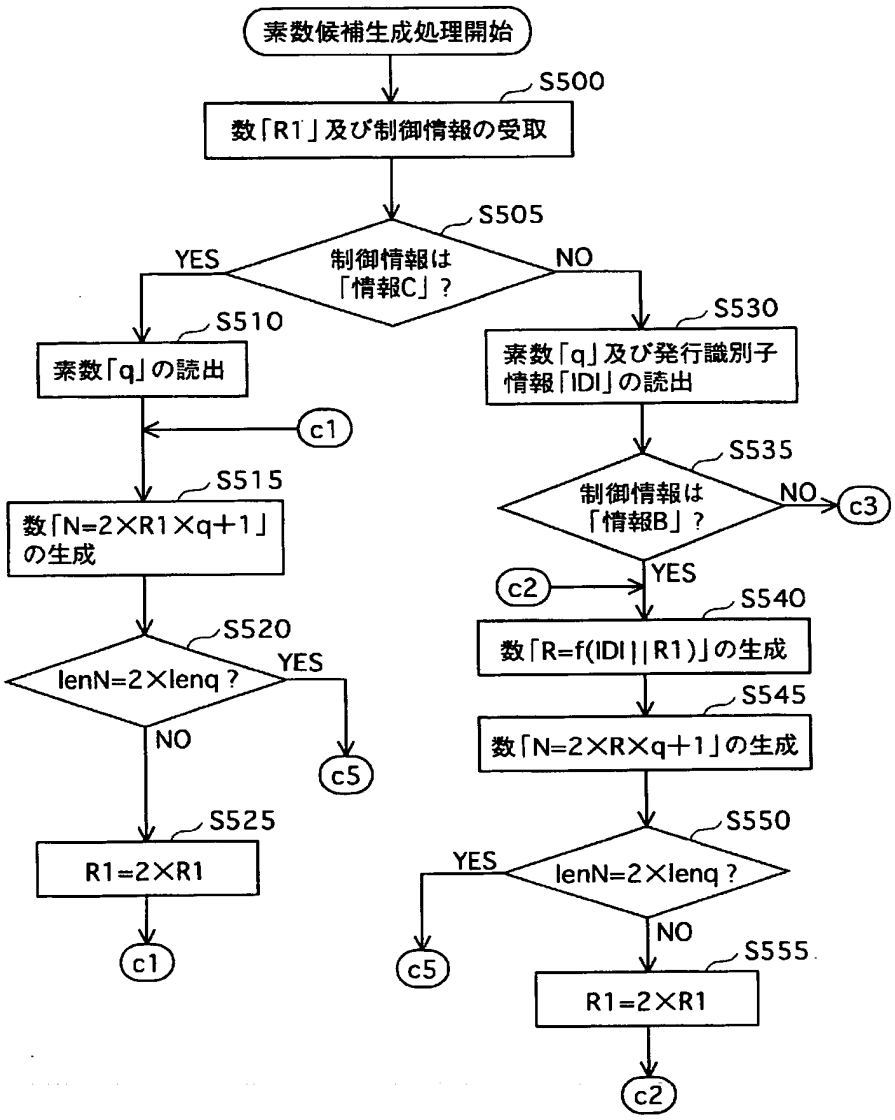
[図14]


a5
S345
公開鍵証明書「Cert」の受取及び書込
S350
秘密鍵「SK」、公開鍵証明書「Cert」及び端末識別子の取得
S355
「SK」及び「Cert」を端末識別子に対応する端末装置300へ送信
終了

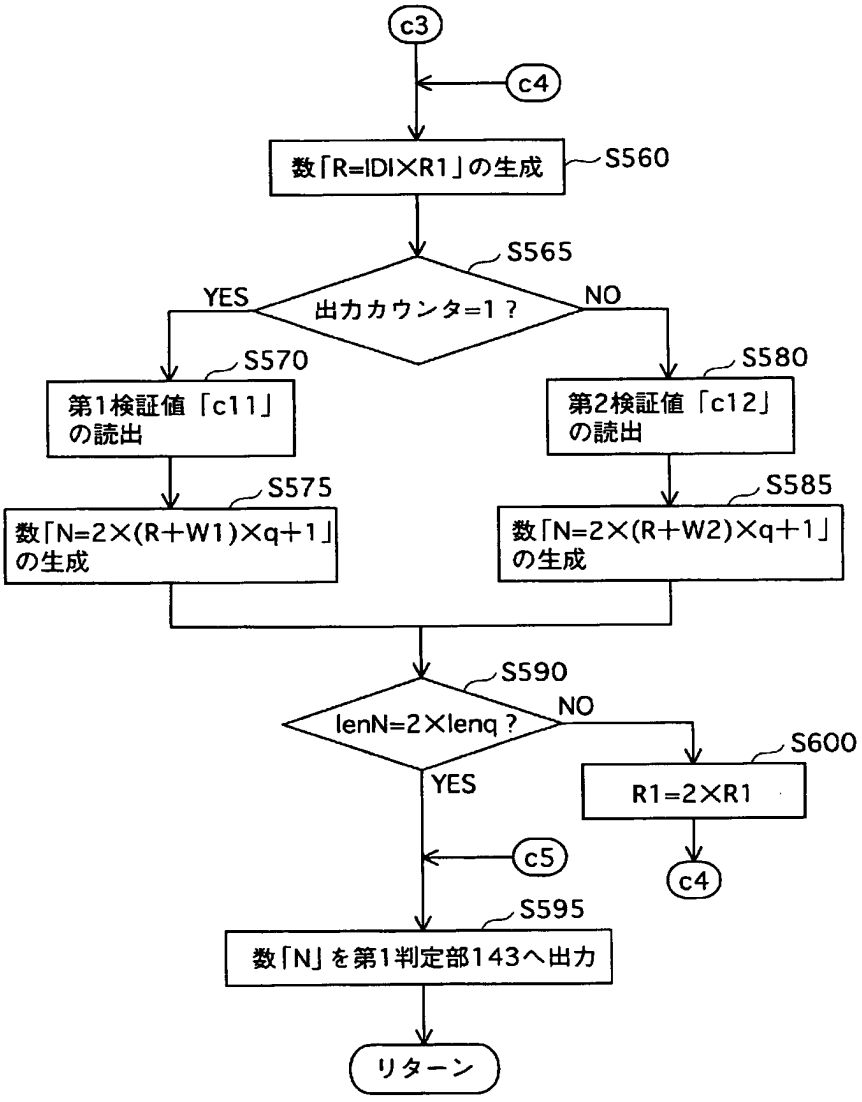
[図15]


素数生成処理開始
S400
情報の受取及び書込
b1
制御情報の読出
S405
S410
制御情報は「情報C」？
YES
NO
S415
「lenq」の読出
S420
(lenq-1)ビットからなる数「R1」を生成
S425
「lenq」及び「lenIDI」の読出
S430
(lenq-lenIDI-1)ビットからなる数「R1」を生成
S435
素数候補生成処理
S440
式(eq1)が成立？
NO
YES
S445
式(eq2)が成立？
NO
YES
S450
生成した数を素数として繰返制御部132へ出力
b1
終了

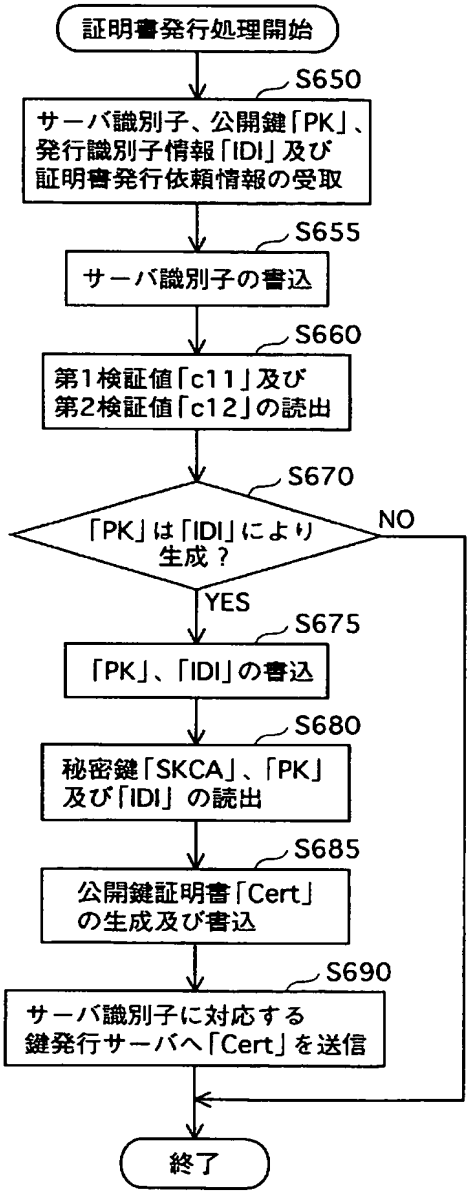
[図16]


素数候補生成処理開始
S500
数「R1」及び制御情報の受取
S505
制御情報は「情報C」？
YES
NO
S510
素数「q」の読出
c1
S515
数「N=2×R1×q+1」の生成
S520
lenN=2×lenq？
YES
NO
c5
S525
R1=2×R1
c1
S530
素数「q」及び発行識別子情報「IDI」の読出
S535
制御情報は「情報B」？
NO
c3
YES
c2
S540
数「R=f(IDI||R1)」の生成
S545
数「N=2×R×q+1」の生成
S550
lenN=2×lenq？
YES
NO
c5
S555
R1=2×R1
c2

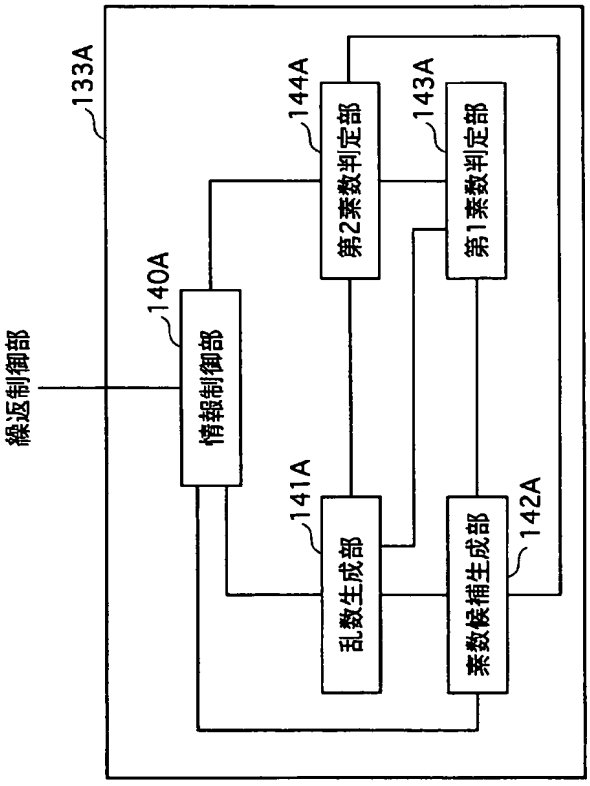
[図17]


c3
c4
数「R=IDI×R1」の生成
S560
S565
出力カウンタ=1？
YES
NO
S570
第1検証値「c11」の読出
S580
第2検証値「c12」の読出
S575
数「N=2×(R+W1)×q+1」の生成
S585
数「N=2×(R+W2)×q+1」の生成
S590
lenN=2×lenq？
NO
S600
R1=2×R1
YES
c5
c4
S595
数「N」を第1判定部143へ出力
リターン

[図18]


証明書発行処理開始
S650
サーバ識別子、公開鍵「PK」、
発行識別子情報「IDI」及び
証明書発行依頼情報の受取
S655
サーバ識別子の書込
S660
第1検証値「c11」及び
第2検証値「c12」の読出
S670
「PK」は「IDI」により
生成？
NO
YES
S675
「PK」、「IDI」の書込
S680
秘密鍵「SKCA」、「PK」
及び「IDI」の読出
S685
公開鍵証明書「Cert」
の生成及び書込
S690
サーバ識別子に対応する
鍵発行サーバへ「Cert」を送信
終了

[図19]

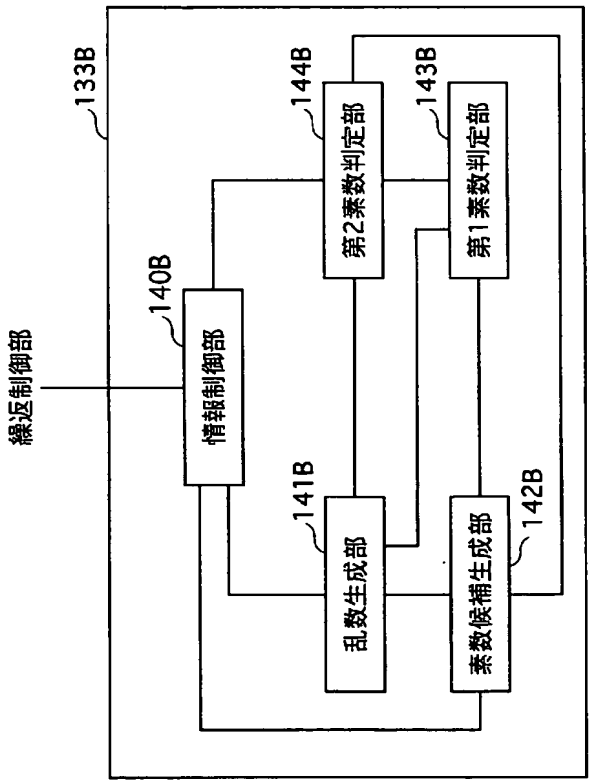

133A
144A
143A
140A
第2素数判定部
第1素数判定部
繰返制御部
情報制御部
141A
142A
乱数生成部
素数候補生成部

[図20]

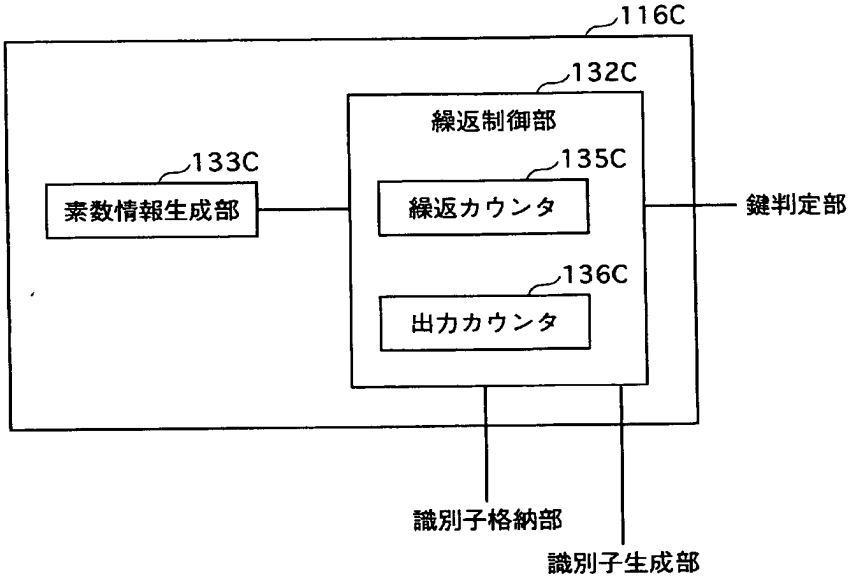
T250

サーバ識別子	検証値
SID A	c1
SID B	c2
SID C	c3

[図21]


133B
144B
143B
140B
第2乗数判定部
第1乗数判定部
繰返制御部
情報制御部
141B
142B
乱数生成部
素数候補生成部

[図22]

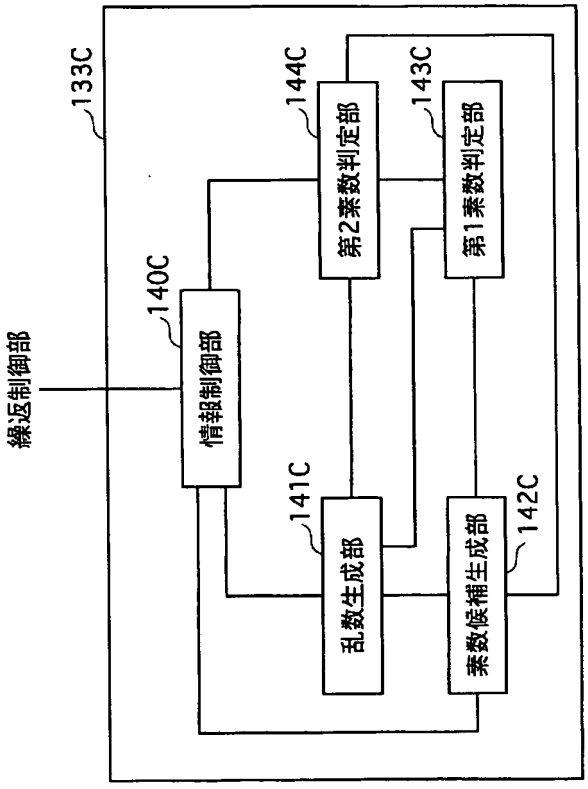

116C
132C
繰返制御部
133C
素数情報生成部
135C
繰返カウンタ
鍵判定部
136C
出力カウンタ
識別子格納部
識別子生成部

[図23]

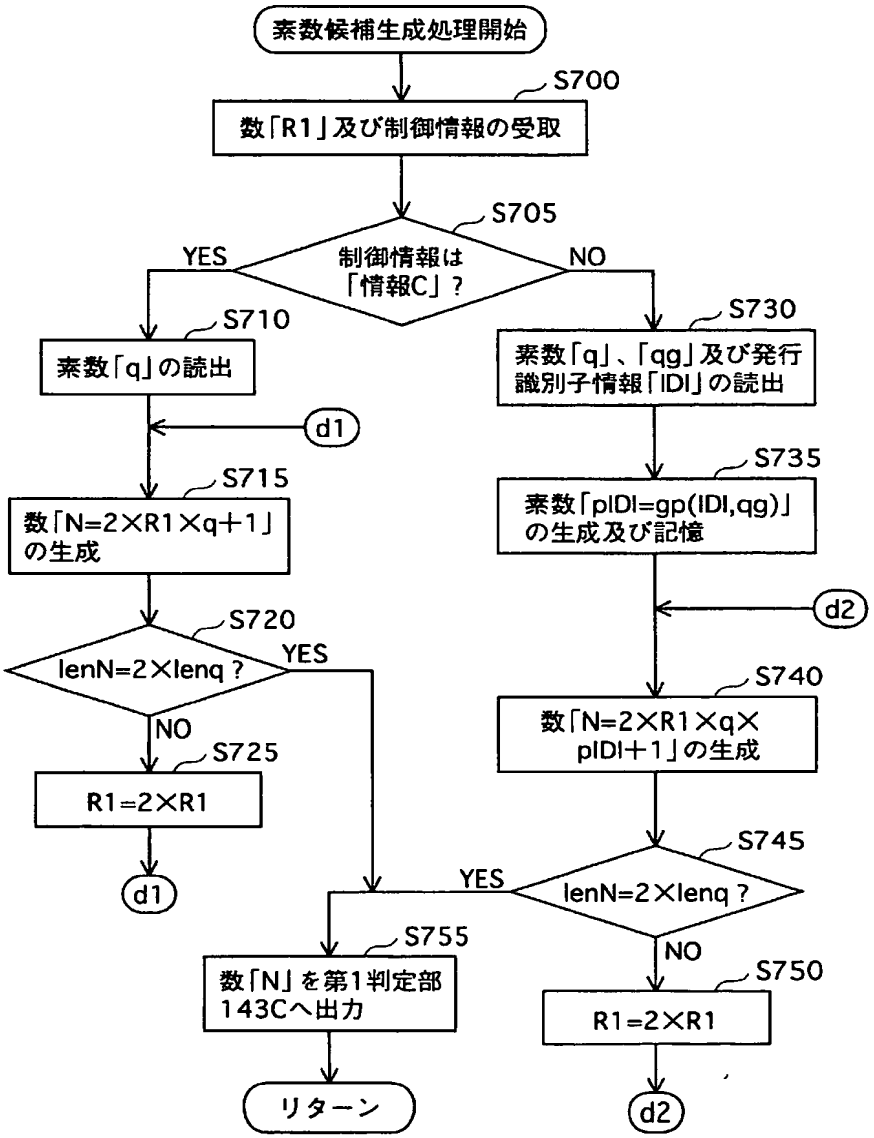
T150

回数	制御情報
1	情報C
2	情報C
3	情報C
4	情報C
5	情報C
6	情報AB

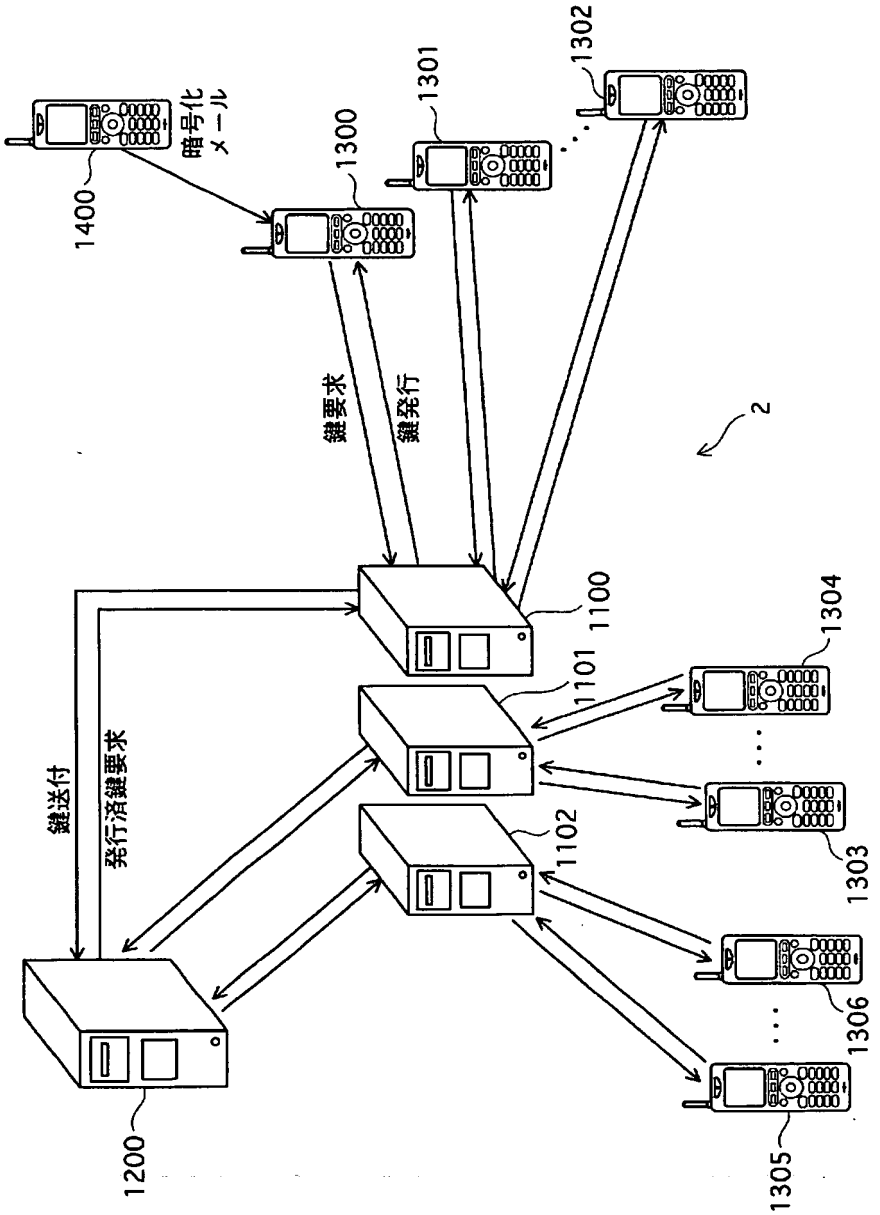
[図24]


133C
144C
143C
140C
第2素数判定部
第1素数判定部
繰返制御部
情報制御部
141C
142C
乱数生成部
素数候補生成部

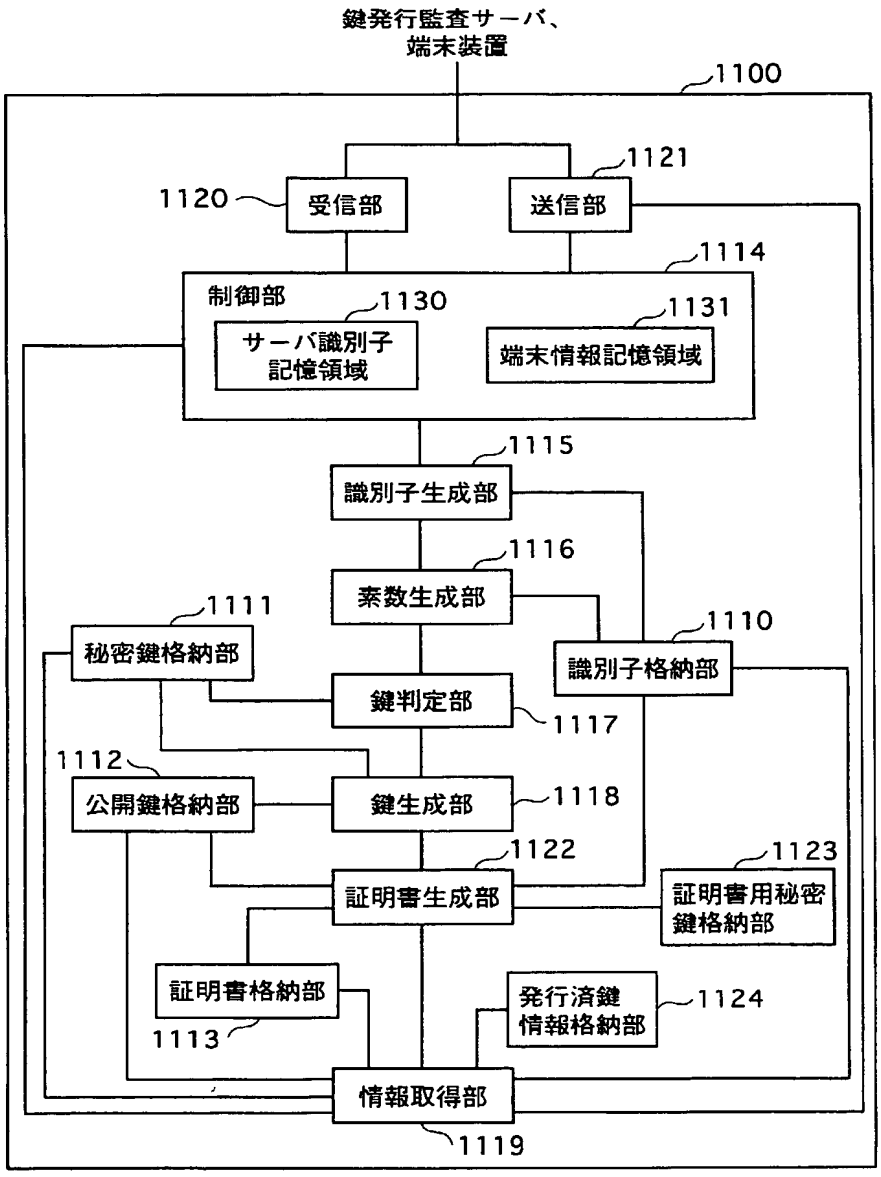
[図25]


素数候補生成処理開始
S700
数「R1」及び制御情報の受取
S705
制御情報は「情報C」？
YES
NO
S710
素数「q」の読出
S730
素数「q」、「qg」及び発行識別子情報「IDI」の読出
d1
S715
数「N=2×R1×q+1」の生成
S735
素数「pIDI=gp(IDI,qg)」の生成及び記憶
d2
S720
lenN=2×lenq？
YES
NO
S740
数「N=2×R1×q×pIDI+1」の生成
S725
R1=2×R1
d1
S745
lenN=2×lenq？
YES
NO
S755
数「N」を第1判定部143Cへ出力
S750
R1=2×R1
リターン
d2

[図26]


暗号化メール
1400
1300
1301
1302
鍵要求
鍵発行
2
1100
1101
1102
1304
1303
1306
1305
鍵送付
発行済鍵要求
1200

[図27]

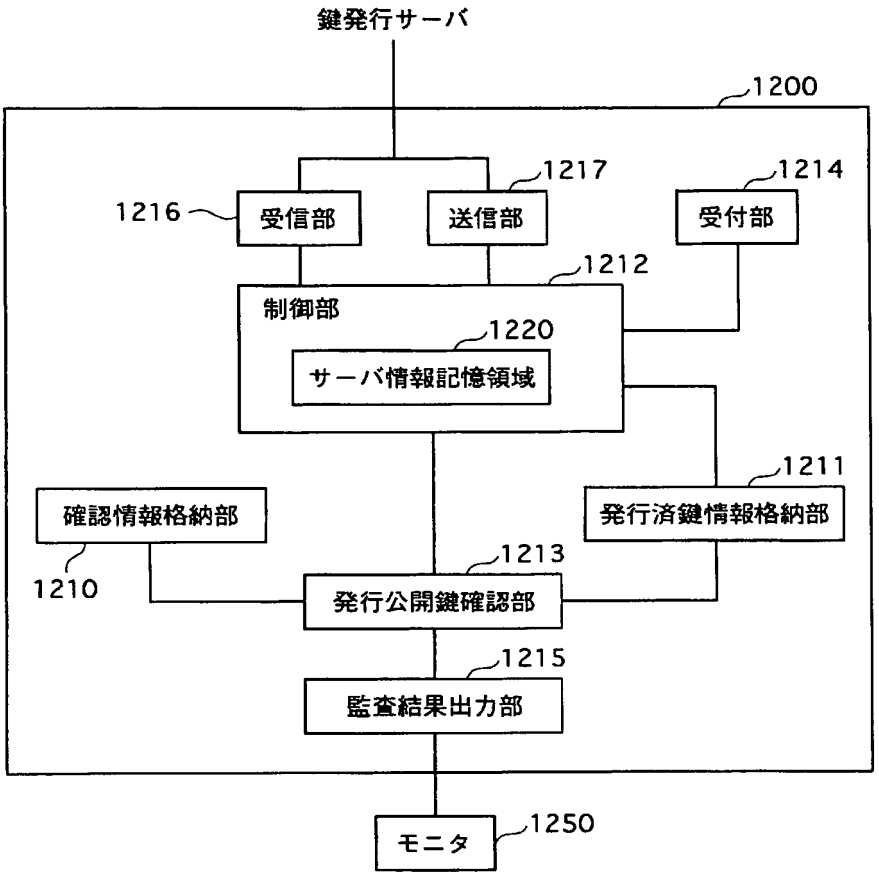

鍵発行監査サーバ、
端末装置
1100
1120
受信部
1121
送信部
1114
制御部
1130
サーバ識別子
記憶領域
1131
端末情報記憶領域
1115
識別子生成部
1116
素数生成部
1111
秘密鍵格納部
1110
識別子格納部
鍵判定部
1117
1112
公開鍵格納部
鍵生成部
1118
1122
1123
証明書生成部
証明書用秘密
鍵格納部
証明書格納部
1113
発行済鍵
情報格納部
1124
情報取得部
1119

[図28]

T1100

発行済公開鍵	発行済識別子情報
PK 1	IDI1
PK 2	IDI 2
⋮	⋮
PK	IDI

[図29]

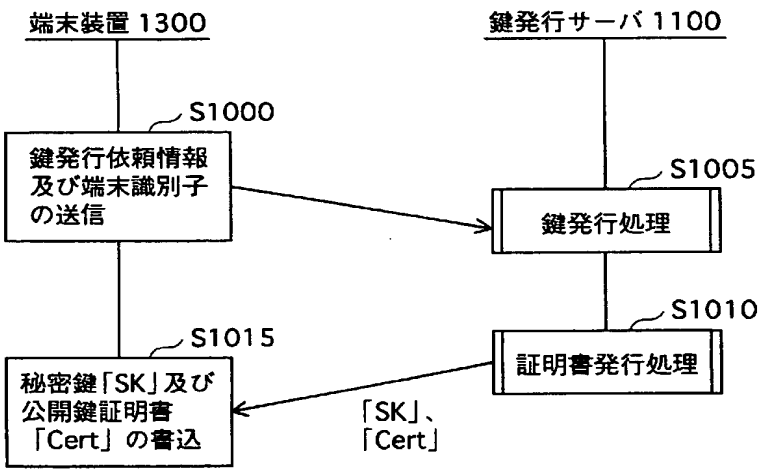

鍵発行サーバ
1200
1217
1214
1216
受信部
送信部
受付部
1212
制御部
1220
サーバ情報記憶領域
1211
確認情報格納部
発行済鍵情報格納部
1210
1213
発行公開鍵確認部
1215
監査結果出力部
モニタ
1250

[図30]

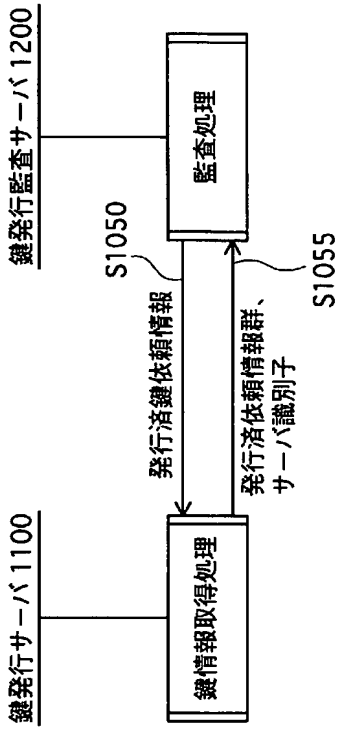
T1200

サーバ識別子	第1検証値	第2検証値
SID A	c11	c12
SID B	c21	c22
SID C	c31	c33

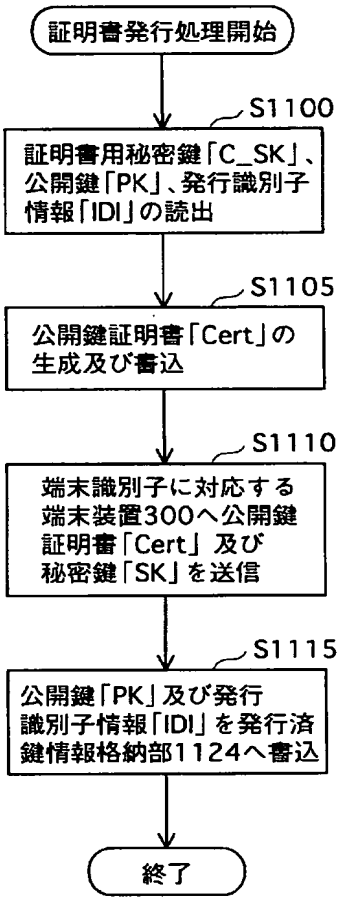
[図31]


端末装置 1300
鍵発行サーバ 1100
S1000
鍵発行依頼情報及び端末識別子の送信
S1005
鍵発行処理
S1010
証明書発行処理
S1015
秘密鍵「SK」及び公開鍵証明書「Cert」の書込
「SK」、「Cert」

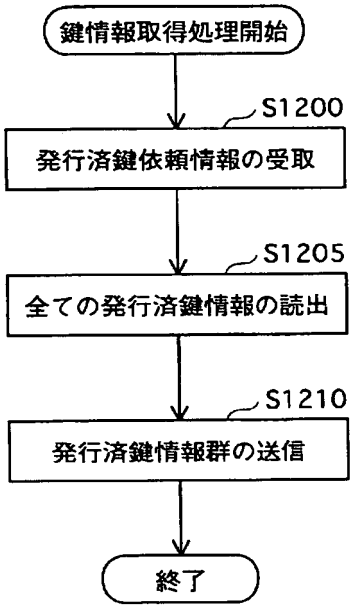
[図32]


鍵発行監査サーバ1200
監査処理
S1050
発行済鍵依頼情報
S1055
発行済依頼情報群、
サーバ識別子
鍵発行サーバ1100
鍵情報取得処理

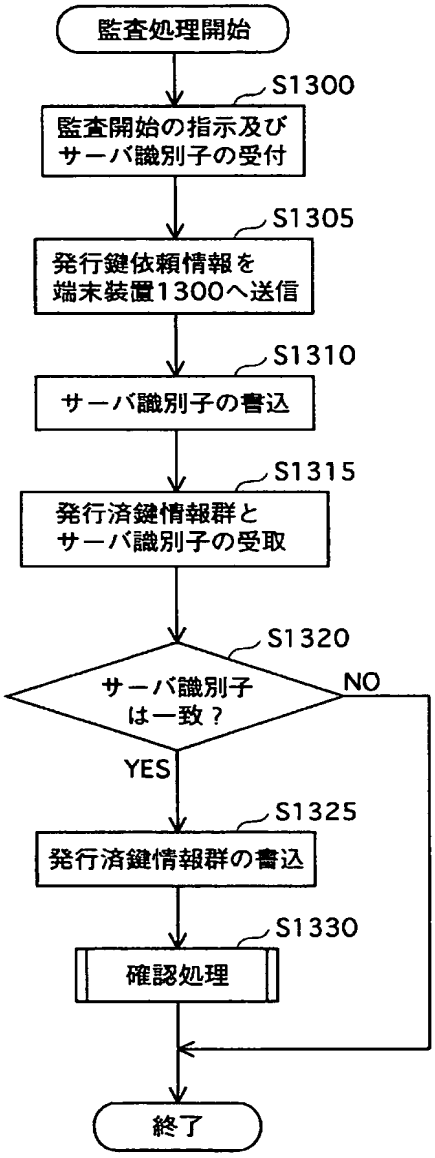
[図33]


証明書発行処理開始
S1100
証明書用秘密鍵「C_SK」、公開鍵「PK」、発行識別子情報「IDI」の読出
S1105
公開鍵証明書「Cert」の生成及び書込
S1110
端末識別子に対応する端末装置300へ公開鍵証明書「Cert」及び秘密鍵「SK」を送信
S1115
公開鍵「PK」及び発行識別子情報「IDI」を発行済鍵情報格納部1124へ書込
終了

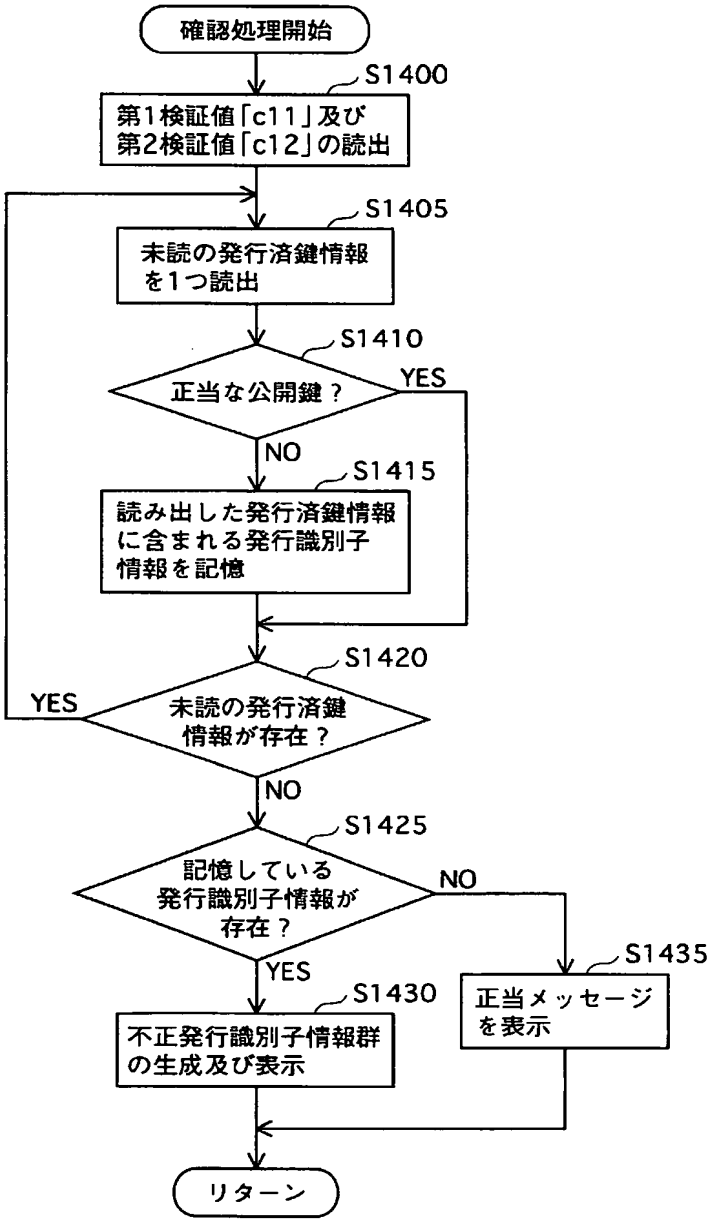
[図34]


鍵情報取得処理開始
S1200
発行済鍵依頼情報の受取
S1205
全ての発行済鍵情報の読出
S1210
発行済鍵情報群の送信
終了

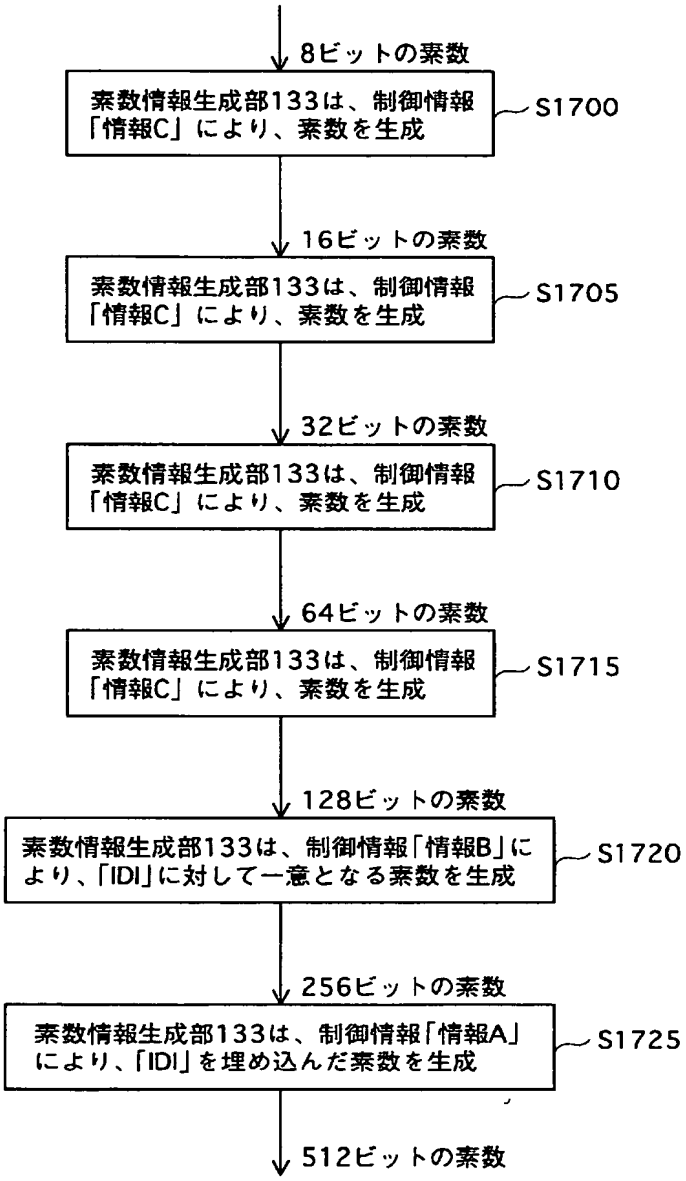
[図35]


監査処理開始
S1300
監査開始の指示及び
サーバ識別子の受付
S1305
発行鍵依頼情報を
端末装置1300へ送信
S1310
サーバ識別子の書込
S1315
発行済鍵情報群と
サーバ識別子の受取
S1320
サーバ識別子
は一致？
NO
YES
S1325
発行済鍵情報群の書込
S1330
確認処理
終了

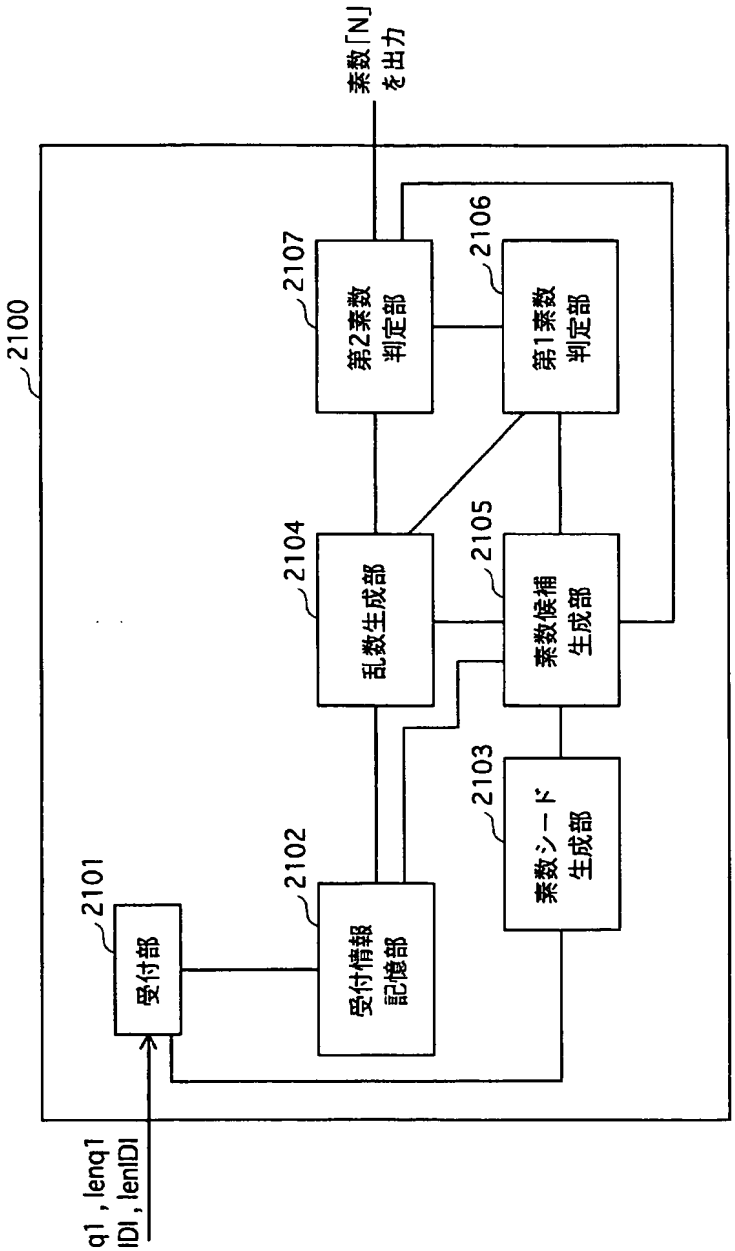
[図36]


確認処理開始
S1400
第1検証値「c11」及び
第2検証値「c12」の読出
S1405
未読の発行済鍵情報
を1つ読出
S1410
正当な公開鍵？
YES
NO
S1415
読み出した発行済鍵情報
に含まれる発行識別子
情報を記憶
S1420
未読の発行済鍵
情報が存在？
YES
NO
S1425
記憶している
発行識別子情報が
存在？
NO
YES
S1430
不正発行識別子情報群
の生成及び表示
S1435
正当メッセージ
を表示
リターン

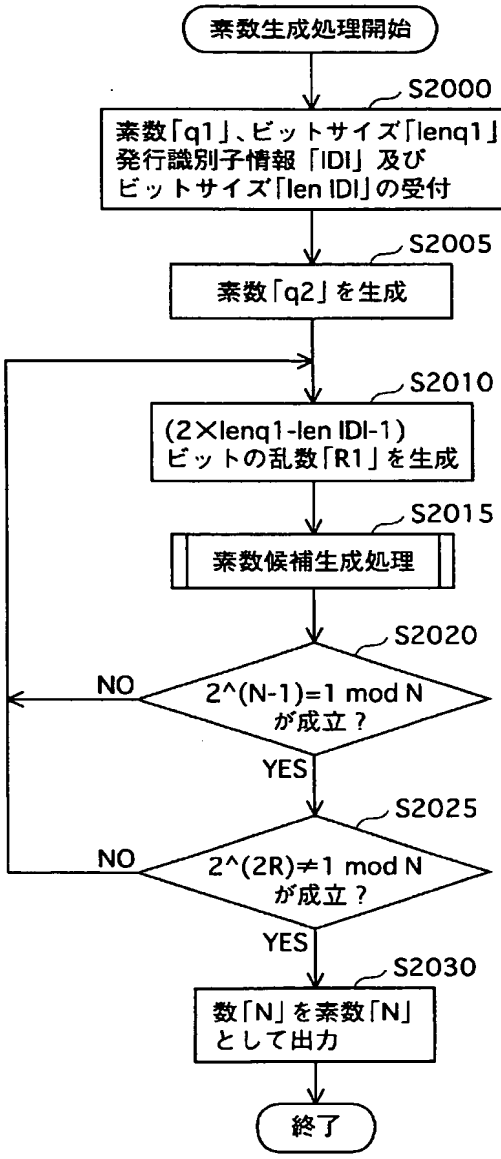
[図37]


8ビットの素数
素数情報生成部133は、制御情報「情報C」により、素数を生成
S1700
16ビットの素数
素数情報生成部133は、制御情報「情報C」により、素数を生成
S1705
32ビットの素数
素数情報生成部133は、制御情報「情報C」により、素数を生成
S1710
64ビットの素数
素数情報生成部133は、制御情報「情報C」により、素数を生成
S1715
128ビットの素数
素数情報生成部133は、制御情報「情報B」により、「IDI」に対して一意となる素数を生成
S1720
256ビットの素数
素数情報生成部133は、制御情報「情報A」により、「IDI」を埋め込んだ素数を生成
S1725
512ビットの素数

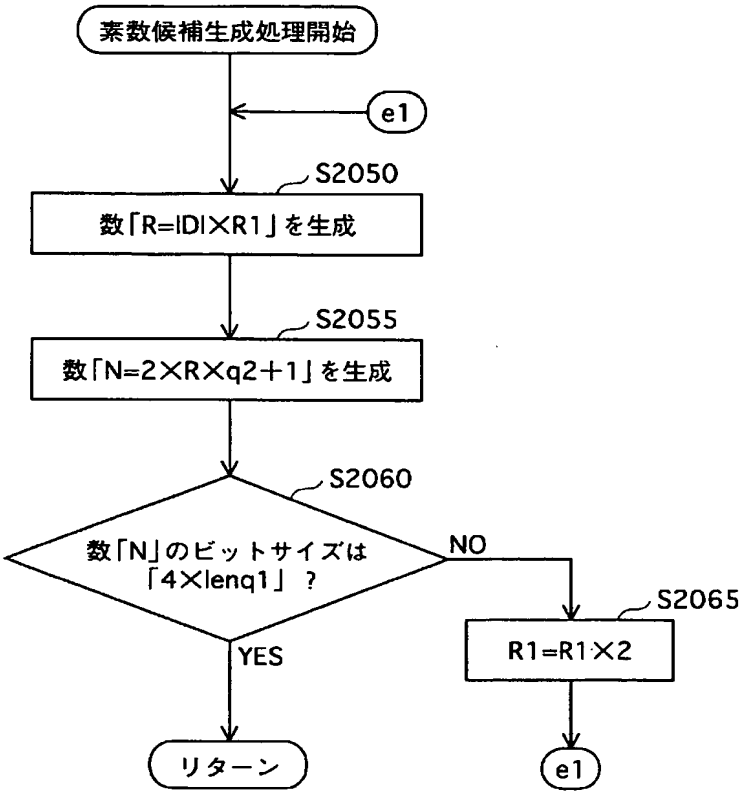
[図38]


素数[N]を出力
2100
2107
第2素数判定部
2106
第1素数判定部
2104
乱数生成部
2105
素数候補生成部
2103
素数シード生成部
2102
受付情報記憶部
2101
受付部
q1 , lenq1
IDI , lenIDI

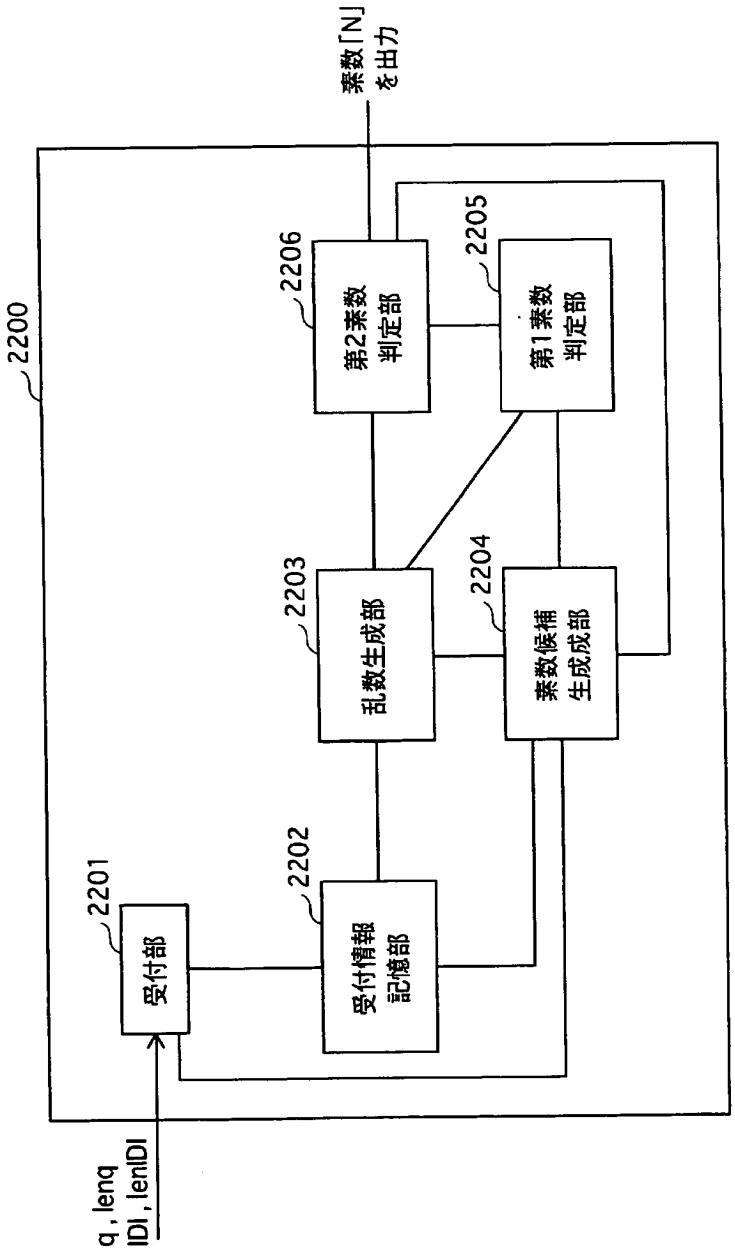
[図39]


素数生成処理開始
S2000
素数「q1」、ビットサイズ「lenq1」、
発行識別子情報「IDI」及び
ビットサイズ「len IDI」の受付
S2005
素数「q2」を生成
S2010
(2×lenq1-len IDI-1)
ビットの乱数「R1」を生成
S2015
素数候補生成処理
S2020
NO
2^(N-1)=1 mod N
が成立？
YES
S2025
NO
2^(2R)≠1 mod N
が成立？
YES
S2030
数「N」を素数「N」
として出力
終了

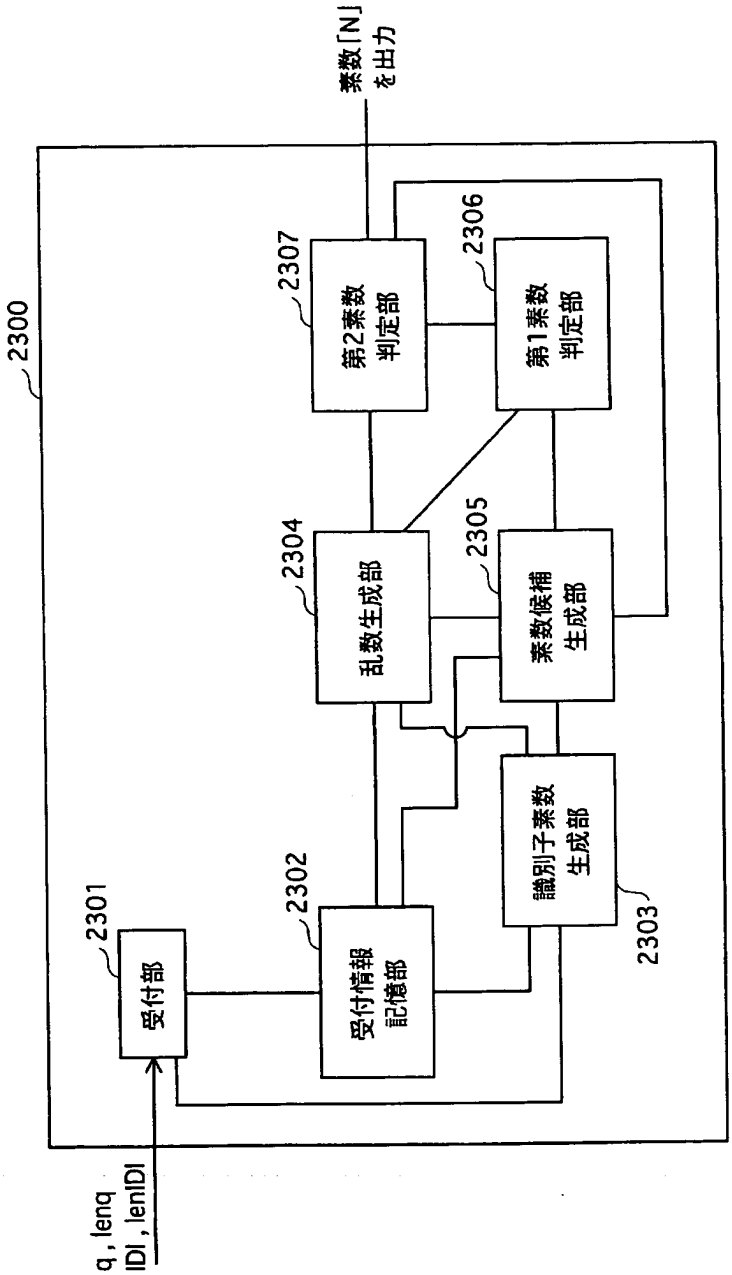
[図40]


素数候補生成処理開始
e1
S2050
数「R=IDI×R1」を生成
S2055
数「N=2×R×q2+1」を生成
S2060
数「N」のビットサイズは
「4×lenq1」？
NO
S2065
R1=R1×2
YES
リターン
e1

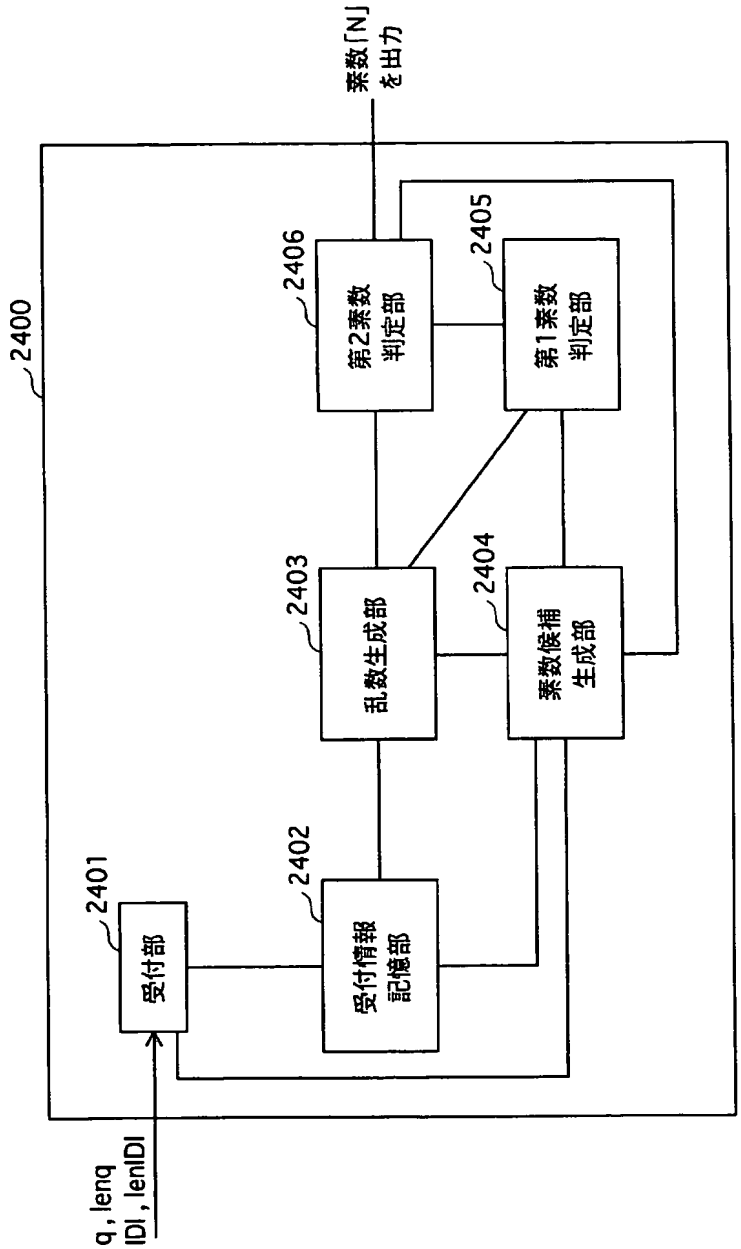
[図41]


素数「N」を出力
2200
2206
第2素数判定部
2205
第1素数判定部
2203
乱数生成部
2204
素数候補生成部
2202
受付情報記憶部
2201
受付部
q, lenq
IDI, lenIDI

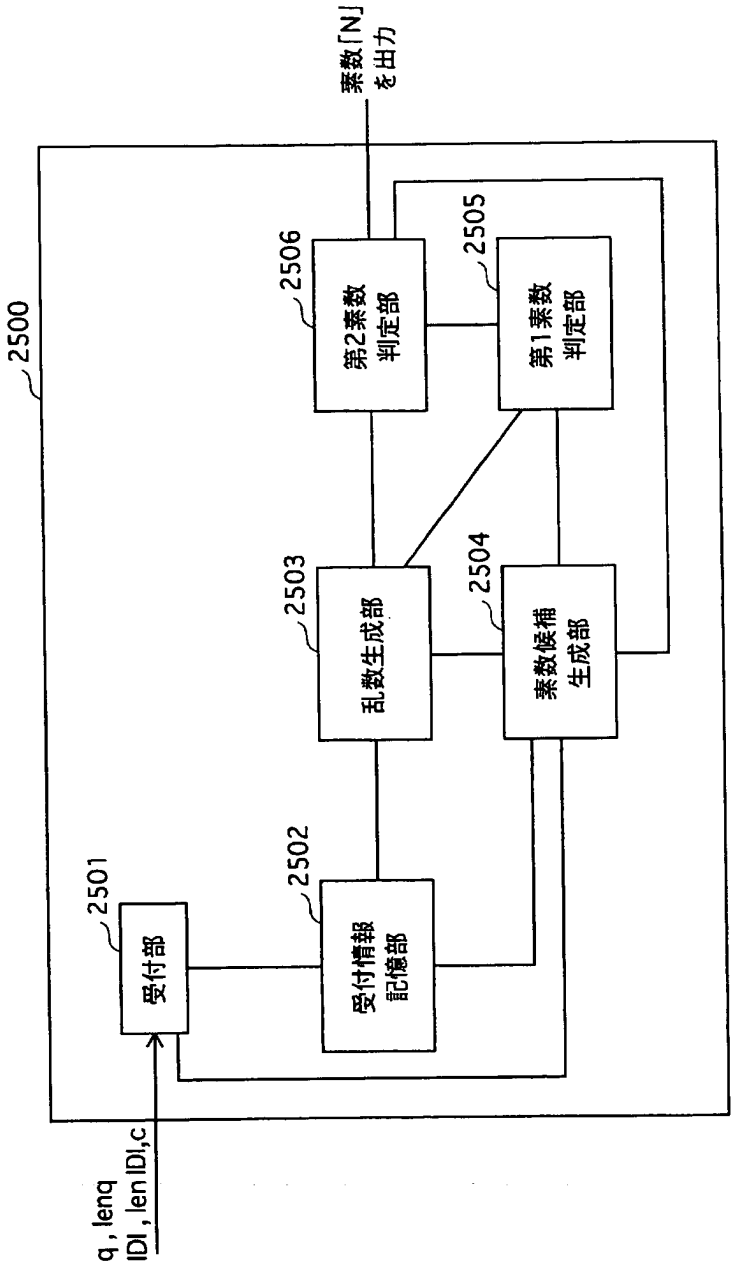
[図42]


素数[N]を出力
2300
2307
第2素数判定部
2306
第1素数判定部
2304
乱数生成部
2305
素数候補生成部
識別子素数生成部
2303
2302
受付情報記憶部
2301
受付部
q, lenq
IDI, lenIDI

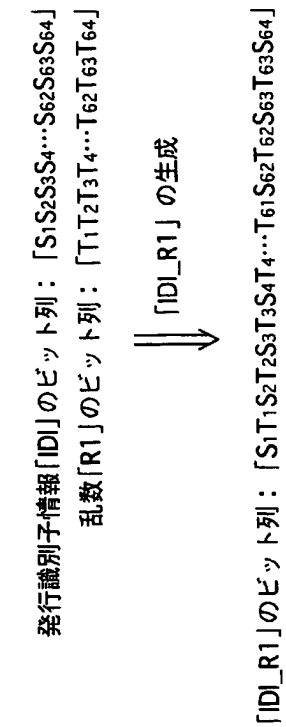
[図43]


素数「N」を出力
2400
2406
第2素数判定部
2405
第1素数判定部
2403
乱数生成部
2404
素数候補生成部
2402
受付情報記憶部
2401
受付部
q, lenq
IDI, lenIDI

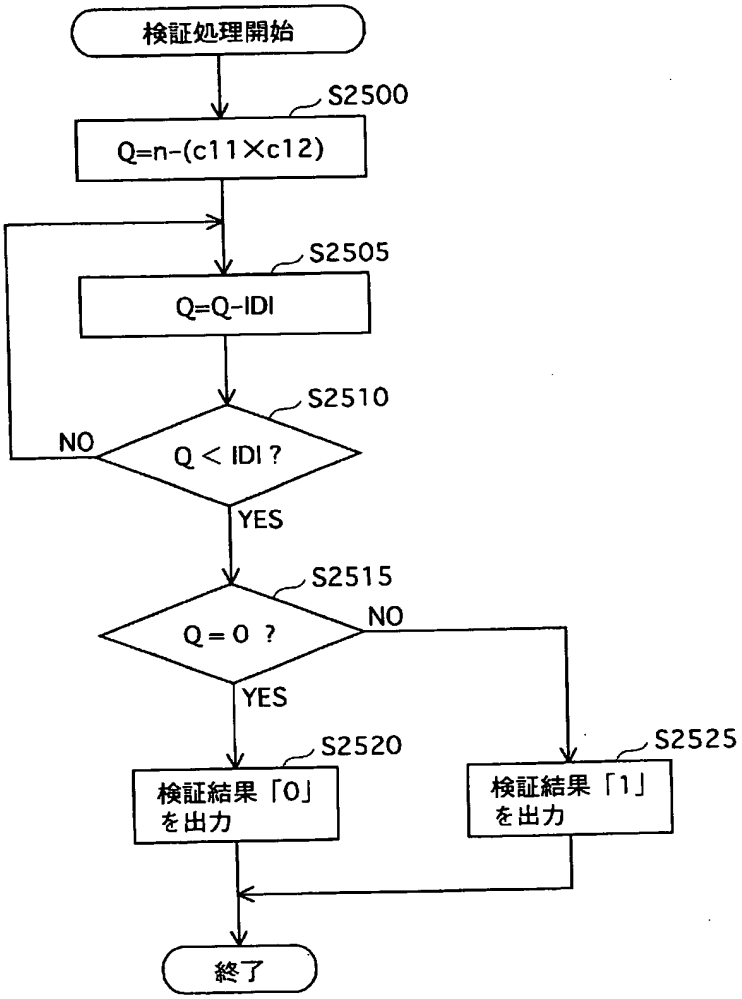
[図44]


素数「N」を出力
2500
2506
第2素数判定部
2505
第1素数判定部
2503
乱数生成部
2504
素数候補生成部
2502
受付情報記憶部
2501
受付部
q, lenq
IDI, len IDI,c

[図45]


発行識別子情報「IDI」のビット列：「S1S2S3S4…S62S63S64」
乱数「R1」のビット列：「T1T2T3T4…T62T63T64」
「IDI_R1」の生成
「IDI_R1」のビット列：「S1T1S2T2S3T3S4T4…T61S62T62S63T63S64」

[図46]


検証処理開始
S2500
Q=n-(c11×c12)
S2505
Q=Q-IDI
S2510
NO
Q < IDI ?
YES
S2515
Q = 0 ?
NO
YES
S2520
検証結果「0」を出力
S2525
検証結果「1」を出力
終了

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2004/019108

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] H04L9/08, G09C1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] H04L9/08, G09C1/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2005
Kokai Jitsuyo Shinan Koho	1971-2005	Toroku Jitsuyo Shinan Koho	1994-2005

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
JSTPLUS FILE(JOIS), WPI(DIALOG), SOSU, SEISEI (in Japanese)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	Generation of RSA Keys That Are Guaranteed to be Unique for Each User, Computer Security, Vol.19, No.3, pages 282 to 288, 2000, particularly, 3. User-Dependent RSA Key Generation	1-23
A	WO 99/52241 A2 (CITIBANK, N.A.), 30 March, 1999 (30.03.99), All pages; particularly, page 5, lines 19 to 30 & AU 9950789 A & EP 1068696 A2 & JP 2002-510810 A & US 6404890 B1 & US 2002/154768 A1 & US 6496929 B2	1-23

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search 18 April, 2005 (18.04.05)	Date of mailing of the international search report 10 May, 2005 (10.05.05)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2004/019108

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 1026851 A1 (Hewlett-Pacakard Co.), 09 August, 2000 (09.08.00), Particularly, Par. Nos. [0012], [0055] to [0060] (Family: none)	1-23
A	JP 7-121107 A (NEC Corp.), 12 May, 1995 (12.05.95), Particularly, Par. Nos. [0008] to [0019] (Family: none)	1-23
A	Fast Generation of Secure RSA-Moduli with Almost Maximal Diversity, Lecture Notes in Computer Science, Vol.434, pages 636 to 641, 1990, particularly, 2. Theoretical Results on the Decipherability by Multiple Encryption, 3. Recursive Algorithm for Generating Cryptographically Secure Primes and RSA-Moduli with Almost Maximal Diversity	1-23
E,A	US 6687375 B1 (International Business Machines Corp.), 03 February, 2004 (03.02.04), All pages (Family: none)	1-23

国際調査報告

国際出願番号 PCT／JP2004／019108

A. 発明の属する分野の分類（国際特許分類（IPC））

Int.Cl.[7] H04L9/08, G09C1/00

B. 調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int.Cl.[7] H04L9/08, G09C1/00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922－1996年
日本国公開実用新案公報	1971－2005年
日本国実用新案登録公報	1996－2005年
日本国登録実用新案公報	1994－2005年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

JSTPLUS ファイル(JOIS), WPI(DIALOG)
素数、生成

C. 関連すると認められる文献

引用文献のカテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
A	Generation of RSA Keys That Are Guaranteed to be Unique for Each User, Computer Security, vol.19 no.3, p.282-288, 2000 特に 3. User-Dependent RSA Key Generation を参照	1-23
A	WO 99/52241 A2 (CITIBANK, N. A.) 1999.03.30 & AU 9950789 A & EP 1068696 A2 & JP 2002-510810 A & US 6404890 B1 & US 2002/154768 A1 & US 6496929 B2 全頁特に第5頁第19-30行を参照	1-23

☑ C欄の続きにも文献が列挙されている。

☐ パテントファミリーに関する別紙を参照。

＊ 引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日 18.04.2005	国際調査報告の発送日 10.5.2005
国際調査機関の名称及びあて先 日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	特許庁審査官（権限のある職員） 5M 9364 中里 裕正 電話番号 03－3581－1101 内線 3599

C（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
A	EP 1026851 A1 (Hewlett-Pacakard Company) 2000.08.09 （ファミリなし）　特に第12, 55-60段落を参照	1-23
A	JP 7-121107 A (日本電気株式会社) 1995.05.12 （ファミリなし）　特に8-19段落を参照	1-23
A	Fast Generation of Secure RSA-Moduli with Almost Maximal Diversity, Lecture Notes in Computer Science, Vol.434, p.636-641 1990 特に2. Theoretical Results on the Decipherability by Multiple Encryption, 3. Recursive Algorithm for Generating Cryptographically Secure Primes and RSA-Moduli with Almost Maximal Diversity を参照	1-23
EA	US 6687375 B1 (International Business Machines Corporation) 2004.02.03 （ファミリなし）全頁を参照	1-23